

STAATSCOURANT

Officiële uitgave van het Koninkrijk der Nederlanden sinds 1814.

Nr. 10213
29 februari
2016

Advies Raad van State inzake het voorstel van wet tot wijziging van de Telecommunicatiewet, de Boeken 3 en 6 van het Burgerlijk Wetboek, de Algemene wet bestuursrecht alsmede daarmee samenhangende wijzigingen van andere wetten in verband met de uitvoering van de EU-verordening elektronische identiteiten en vertrouwensdiensten (uitvoering EU-verordening elektronische identiteiten en vertrouwensdiensten)

Nader Rapport

's-Gravenhage, 17 februari 2016
Nr. WJZ / 16019493

Aan de Koning

Nader rapport inzake het voorstel van wet tot wijziging van de Telecommunicatiewet, de Boeken 3 en 6 van het Burgerlijk Wetboek, de Algemene wet bestuursrecht alsmede daarmee samenhangende wijzigingen van andere wetten in verband met de uitvoering van de EU-verordening elektronische identiteiten en vertrouwensdiensten (uitvoering EU-verordening elektronische identiteiten en vertrouwensdiensten)

Blijkens de mededeling van de Directeur van Uw kabinet van 16 december 2015, nr. 2015002235, machtigde Uwe Majesteit de Afdeling advisering van de Raad van State haar advies inzake het bovenvermelde voorstel van wet rechtstreeks aan mij te doen toekomen. Dit advies, gedateerd 4 februari 2016, nr. W15.15/0442/IV, bied ik U hierbij aan.

Het laatste lid van het laatste artikel van het wetsvoorstel verklaart artikel 12 van de Wet raadgevend referendum op de inwerkingtreding van het wetsvoorstel van toepassing. De Afdeling wijst er terecht op dat er geen noodzaak bestaat om dit artikellid van toepassing te verklaren, ook niet indien dit zou beogen te anticiperen op de situatie dat in de parlementaire behandeling onderwerpen aan het wetsvoorstel worden toegevoegd die de verplichte uitvoering van de verordening te buiten gaan. Het wetsvoorstel strekt uitsluitend tot omzetting van de verordening, zodat het advies van de Afdeling tot schrappen van het desbetreffende artikellid is overgenomen en verwerkt in het wetsvoorstel.

In onderdeel I van het wetsvoorstel is in artikel 15.1 een wijziging van technische aard aangebracht. De memorie van toelichting is hierop aangepast. Paragraaf 5.8 van het algemeen deel van memorie van toelichting is voorts op het specifieke punt van conformiteitsbeoordelingen aangevuld, onder meer door aan een nieuwe norm voor conformiteitsbeoordelingsinstanties te refereren (paragraaf 5.8). Daarnaast bevat de toelichting op artikel I, onderdeel Q, artikel 18.15b, ter verduidelijking een aanvulling op wat identiteitsverificatie van een natuurlijke persoon bij de afgifte van een gekwalificeerd certificaat in de praktijk betekent. In de artikelsgewijze toelichting is verder de toelichting op artikel II aangevuld door daarin aan te geven dat partijen afspraken kunnen blijven maken over het betrouwbaarheidsniveau van geavanceerde en andere elektronische handtekeningen, uitgezonderd gekwalificeerde elektronische handtekeningen. Tot slot is in de artikelen XII tot en met XIV voorzien in verschillende situaties waarin technische samenloop kan optreden met andere wetsvoorstellen of nog in werking te treden wetten en is de memorie van toelichting daarop aangepast. Het betreft het wetsvoorstel tot wijziging van het Wetboek van Burgerlijke rechtsvordering en de Algemene wet bestuursrecht in verband met vereenvoudiging en digitalisering van het procesrecht (Kamerstukken I en II, 34 059) en verscheidene wetsvoorstellen en nog in werking te treden wetten die de Telecommunicatiewet wijzigen.

Ik moge U verzoeken, mede namens de Minister van Veiligheid en Justitie en de Minister van Binnenlandse Zaken en Koninkrijksrelaties, het hierbij gevoegde gewijzigde voorstel van wet en de gewijzigde memorie van toelichting aan de Tweede Kamer der Staten-Generaal te zenden.

De Minister van Economische Zaken,
H.G.J. Kamp.



Advies Raad van State

No.W15.15.0442/IV
's-Gravenhage, 4 februari 2016

Aan de Koning

Bij Kabinetsmissive van 16 december 2015, no.2015002235, heeft Uwe Majesteit, op voordracht van de Minister van Economische Zaken, mede namens de Minister van Binnenlandse Zaken en Koninkrijksrelaties en de Minister van Veiligheid en Justitie, bij de Afdeling advisering van de Raad van State ter overweging aanhangig gemaakt het voorstel van wet tot wijziging van de Telecommunicatiewet, de Boeken 3 en 6 van het Burgerlijk Wetboek, de Algemene wet bestuursrecht alsmede daarmee samenhangende wijzigingen van andere wetten in verband met de uitvoering van EU-verordening elektronische identiteiten en vertrouwensdiensten (uitvoering EU-verordening elektronische identiteiten en vertrouwensdiensten), met memorie van toelichting.

Het wetsvoorstel geeft uitvoering aan de onderdelen van de EU-verordening elektronische identiteiten en vertrouwensdiensten (hierna: de verordening), die noodzaken tot wetswijziging.[1] De verordening regelt grensoverschrijdend gebruik van elektronische identificatiemiddelen en vertrouwensdiensten tussen EU-lidstaten en zal vanaf 1 juli 2016 rechtstreeks van toepassing zijn.

De Afdeling advisering van de Raad van State adviseert het voorstel naar de Tweede Kamer te zenden, maar acht aanpassing van het voorstel wenselijk. Nu er geen noodzaak bestaat om artikel 12 van de Wet raadgevend referendum (Wrr) op de inwerkingtreding van het voorstel van toepassing te verklaren dient de desbetreffende bepaling uit het voorstel te worden geschrapt.

Het voorgestelde artikel XII regelt inwerkingtreding van het wetsvoorstel op een bij koninklijk besluit te bepalen tijdstip. Daarbij kan de inwerkingtreding voor verschillende artikelen of onderdelen daarvan verschillend worden vastgesteld. Het tweede lid van artikel XII bepaalt dat in het inwerkingtredingsbesluit zo nodig toepassing wordt gegeven aan artikel 12 van de Wet raadgevend referendum bij de inwerkingtreding van artikelen of onderdelen van het voorstel van wet die zijn gewijzigd na indiening van het voorstel bij de Tweede Kamer. Een toelichting op het tweede lid van artikel XII ontbreekt.

De Afdeling wijst erop dat op grond van artikel 5, onderdeel e, van de Wrr, geen referendum kan worden gehouden over wetten die uitsluitend strekken tot uitvoering van verdragen of besluiten van volkenrechtelijke organisaties. Uit de memorie van toelichting van de Wrr blijkt dat deze uitzondering mede ziet op wetten die uitvoering geven aan Europese verordeningen.[2] Het wetsvoorstel strekt uitsluitend tot omzetting van de verordening.[3] Daardoor is het voorstel op grond van artikel 5, onderdeel e, niet referendabel en is het niet noodzakelijk om artikel 12 Wrr op de inwerkingtreding van toepassing te verklaren.

Voor zover het tweede lid van artikel XII beoogt te anticiperen op de situatie dat in de parlementaire behandeling onderwerpen aan het wetsvoorstel worden toegevoegd die de verplichte uitvoering van de verordening te buiten gaan, merkt de Afdeling het volgende op. Het uitgangspunt bij implementatie van bindende EU regelgeving is dat in de implementatieregeling geen andere regels worden opgenomen dan voor de implementatie noodzakelijk zijn.[4] Dit uitgangspunt geldt ook voor nota's van wijziging en amendementen met betrekking tot het wetsvoorstel. In die zin is het niet nodig en niet wenselijk bij voorbaat een regeling op te nemen voor het geval van dit uitgangspunt zou worden afgeweken.

Daarnaast wijst de Afdeling erop dat het opnemen van een bepaling als het tweede lid van artikel XII geen recht doet aan het uitgangspunt van de Wrr dat artikel 12 uitsluitend in uitzonderingsituaties moet worden toegepast. De reden voor toepassing van artikel 12 Wrr zal, blijkens de toelichting op de Wrr,[5] geen andere kunnen zijn dan dat de wet dermate spoedeisend is dat afgeweken moet worden

[1] Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische certificaten en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG (PbEU 2014, L 257). Ook 'eidas verordening' genoemd.
[2] Kamerstukken II 2005/06, 30 372, nr. 3, paragraaf 7.2.
[3] Zie ook de toelichting, paragraaf 12, eerste zin.
[4] Vergelijk Aanwijzingen voor de regelgeving, Ar 331.
[5] Kamerstukken II 2005/06, 30 372, nr. 3, paragraaf 8.3.2.



van de algemene inwerkingtredingsprocedure uit de artikelen 8 en 9 Wrr.[6] Deze spoedeisendheid dient in zo’n geval dan ook gemotiveerd te worden.[7] Het voor de zekerheid opnemen van een bepaling die artikel 12 Wrr van toepassing verklaart, voor het geval toepassing ervan in de loop van de parlementaire behandeling wenselijk blijkt, voldoet niet aan dit uitgangspunt.

De Afdeling adviseert op grond van het bovenstaande het tweede lid van artikel XII te schrappen.

De Afdeling advisering van de Raad van State geeft U in overweging het voorstel van wet te zenden aan de Tweede Kamer der Staten-Generaal, nadat met het vorenstaande rekening zal zijn gehouden.

De vice-president van de Raad van State,
J.P.H. Donner.

[6] Deze normale procedure houdt in dat het tijdstip van inwerkingtreding van een wet waarover een referendum kan worden gehouden, niet eerder wordt gesteld dan acht weken na de mededeling van de minister van Binnenlandse Zaken en Koninkrijksrelaties over de bekrachtiging van die wet. Deze mededeling wordt binnen een week na die bekrachtiging geplaatst in de Staatscourant.

[7] Zie bijvoorbeeld de adviezen van de Afdeling advisering van de Raad van State van 29 oktober 2015 over het voorstel van wet tot wijziging van de Pensioenwet, de Wet verplichte beroepspensioenregeling en de Wet op de loonbelasting 1964 in verband met invoering van een variabele uitkering (Wet variabele pensioenuitkering) (W12.15.0366/III), Kamerstukken II 2015/16, 34 344, nr. 4 en van 9 december 2015 over het voorstel van wet tot wijziging van Boek 7 van het Burgerlijk Wetboek en enkele andere wetten in verband met het stellen van nadere huurmaatregelen tot verdere bevordering van de doorstroming op de huurmarkt (Wet doorstroming huurmarkt 2015) (W03.15.0379/II), Kamerstukken II 2015/16, 34 373, nr. 4.



Tekst zoals toegezonden aan de Afdeling advisering van de Raad van State: Wet tot wijziging van de Telecommunicatiewet, de Boeken 3 en 6 van het Burgerlijk Wetboek, de Algemene wet bestuursrecht alsmede daarmee samenhangende wijzigingen van andere wetten in verband met de uitvoering van EU-verordening elektronische identiteiten en vertrouwensdiensten (uitvoering EU-verordening elektronische identiteiten en vertrouwensdiensten)

Wij Willem-Alexander, bij de gratie Gods, Koning der Nederlanden, Prins van Oranje-Nassau, enz. enz. enz.

Allen, die deze zullen zien of horen lezen, saluut! doen te weten:

Alzo Wij in overweging genomen hebben, dat het noodzakelijk is Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG (PbEU 2014, L257) uit te voeren, en dat het wenselijk is de hiervoor noodzakelijke bepalingen aan te passen in de Boeken 3 en 6 van het Burgerlijk Wetboek, de Telecommunicatiewet, de Algemene wet bestuursrecht, alsmede daarmee samenhangende wijzigingen van andere wetten;

Zo is het, dat Wij, de Afdeling advisering van de Raad van State gehoord, en met gemeen overleg der Staten-Generaal, hebben goedgevonden en verstaan, gelijk Wij goedvinden en verstaan bij deze:

ARTIKEL I

De Telecommunicatiewet wordt als volgt gewijzigd:

A

Artikel 1.1 wordt als volgt gewijzigd:

a. De onderdelen ss tot en met yy komen te luiden:

ss. *vertrouwensdienst:* een vertrouwensdienst als bedoeld in artikel 3, onderdeel 16, van de eidas-verordening;
tt. *gekwalificeerde vertrouwensdienst:* een vertrouwensdienst als bedoeld in artikel 3, onder 17, van de eidas-verordening;
uu. *verlener van vertrouwensdiensten:* een verlener van vertrouwensdiensten als bedoeld in artikel 3, onderdeel 19, van de eidas-verordening;
vv. *gekwalificeerde verlener van vertrouwensdiensten:* een gekwalificeerde verlener van een vertrouwensdienst als bedoeld in artikel 3, onderdeel 20, van de eidas-verordening;
ww. *gekwalificeerd certificaat:* een gekwalificeerd certificaat voor elektronische handtekeningen als bedoeld in artikel 3, onderdeel 15 van de eidas-verordening, een gekwalificeerd certificaat voor elektronische zegels als bedoeld in artikel 3, onderdeel 30, van de eidas-verordening of een gekwalificeerd certificaat voor websiteauthenticatie als bedoeld in artikel 3, onderdeel 39, van de eidas-verordening;
xx. *conformiteitsbeoordelingsinstantie:* een conformiteitsbeoordelingsinstantie als bedoeld in artikel 3, onderdeel 18, van de eidas-verordening;
yy. *gekwalificeerd middel voor het aanmaken van elektronische handtekeningen of elektronische zegels:* gekwalificeerd middel voor het aanmaken van elektronische handtekeningen als bedoeld in artikel 3, onderdeel 23, van de eidas-verordening of voor het aanmaken van elektronische zegels als bedoeld in artikel 3 onderdeel 32, van de eidas-verordening;

b. Onder vervanging van de punt aan het slot van onderdeel kkk door een puntkomma worden drie onderdelen toegevoegd, luidende:

lll. *toezichthoudend orgaan:* een toezichthoudend orgaan als bedoeld in artikel 17, eerste lid, van de eidas-verordening;
mmm. *vertrouwenslijst:* een vertrouwenslijst als bedoeld in artikel 22 van de eidas-verordening;
nnn. *eidas-verordening:* verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG (PbEU 2014, L 257), en de op grond van die verordening door de Europese Commissie vastgestelde uitvoerings- en gedelegeerde handelingen.



B

In hoofdstuk 2 wordt voor artikel 2.1 een opschrift ingevoegd, luidende:

§ 2.1 Aanleg of aanbieden openbare elektronische communicatienetwerken of -diensten

C

In artikel 2.1 vervallen het vijfde tot en met het zevende lid.

D

Artikel 2.2 wordt als volgt gewijzigd:

a. Het tweede lid komt te luiden:

2. De Autoriteit Consument en Markt beëindigt of wijzigt de registratie indien de grond voor registratie is vervallen.

b. Het derde tot en met vijfde lid vervallen.

E

Artikel 2.3 wordt als volgt gewijzigd:

a. In het eerste lid wordt na ‘een register van de registraties’ ingevoegd: , bedoeld in artikel 2.1, vierde lid,.

b. Het derde en vierde lid vervallen onder vernummering van het vijfde tot en met zevende lid tot het derde tot en met vijfde lid.

c. In het derde lid (nieuw) vervalt: of op de in het register opgenomen gegevens die krachtens het vierde lid zijn verstrekt.

d. In het vierde lid (nieuw) wordt ‘artikel 2.2, vierde lid’ vervangen door ‘artikel 2.2, tweede lid’ en ‘op grond van het vijfde lid’ door: op grond van het derde lid.

e. In het vijfde lid (nieuw) wordt ‘het zesde lid’ vervangen door: het vierde lid.

F

Na artikel 2.5 wordt een paragraaf ingevoegd, luidende:

§ 2.2. Het verlenen van vertrouwensdiensten

Artikel 2.5a

Deze wet is niet van toepassing op de verlening van vertrouwensdiensten of op het voornemen tot verlening daarvan, die van het toepassingsbereik van de eidas-verordening zijn uitgesloten.

Artikel 2.5b

1. Een mededeling van een verlener van vertrouwensdiensten aan Onze Minister waaruit het voornemen tot het verlenen van gekwalificeerde vertrouwensdiensten blijkt, wordt aangemerkt als een aanvraag tot toekenning van de status gekwalificeerd aan die verlener en de door hem in die mededeling aangeduide vertrouwensdiensten.

2. Onze Minister neemt een aanvraag als bedoeld in het eerste lid niet in behandeling, indien de aanvrager buiten Nederland gevestigd is.

3. Onze Minister kan bij ministeriële regeling bepalen welke andere gegevens dan de overlegging van een conformiteitsbeoordelingsverslag als bedoeld in artikel 21, eerste lid, van de eidas-verordening bij een aanvraag dienen te worden overgelegd en de wijze van verstrekking daarvan.

4. Een beschikking op een aanvraag als bedoeld in het eerste lid, wordt gegeven binnen de

termijn van drie maanden, bedoeld in artikel 21, tweede lid, van de eidas-verordening.

Artikel 2.5c

1. Onze Minister draagt zorg voor het opstellen en bijhouden van een langs elektronische weg openbaar toegankelijke vertrouwenslijst ten aanzien van in Nederland gevestigde gekwalificeerde verleners van vertrouwensdiensten en van de door hen te verlenen gekwalificeerde vertrouwensdiensten.

2. Indien als gevolg van een wijziging van de eidas-verordening de op de vertrouwenslijst te vermelden gegevens aangepast dienen te worden, verstrekt een gekwalificeerde verlener van vertrouwensdiensten onverwijld aan Onze Minister de gegevens voor opname in de vertrouwenslijst die aanpassing mogelijk maken.

3. Een gekwalificeerde verlener van vertrouwensdiensten geeft aan Onze Minister onverwijld alle wijzigingen door die van invloed zijn op zijn status van gekwalificeerd, op het gekwalificeerd zijn van de door hem te verlenen vertrouwensdiensten of op de in de vertrouwenslijst over hem of zijn te verlenen diensten opgenomen gegevens.

4. Onze Minister brengt de vertrouwenslijst in overeenstemming met de wijzigingen die voortvloeien uit artikel 2.5d of met wijzigingen die Onze Minister op grond van het tweede of derde lid heeft ontvangen.

5. Een gekwalificeerde verlener van vertrouwensdiensten verstrekt op verzoek van Onze Minister alle gegevens die Onze Minister noodzakelijk acht voor de volledigheid van de inhoud van de vertrouwenslijst.

6. Onze Minister kan gegevens in de vertrouwenslijst wijzigen indien dit noodzakelijk is om feitelijke onjuistheden van eenvoudige aard weg te nemen.

7. Indien dit voor een goede uitvoering van de eidas-verordening vereist is, worden bij ministeriële regeling regels gesteld over:
   a. het opstellen, bijhouden en publiceren van de vertrouwenslijst;
   b. de door een gekwalificeerde verlener van vertrouwensdiensten aan Onze Minister te overleggen gegevens voor de vertrouwenslijst en de wijze van aanlevering daarvan.

Artikel 2.5d

1. Onze Minister kan onverminderd artikel 20, derde lid, van de eidas-verordening, tot beëindiging van de status gekwalificeerd overgaan:
   a. indien een gekwalificeerde verlener van vertrouwensdiensten in strijd met het bepaalde bij of krachtens deze wet handelt ten aanzien van het verlenen van vertrouwensdiensten;
   b. indien hij heeft vastgesteld dat de gekwalificeerde verlener van vertrouwensdiensten de gegevens, bedoeld in artikel 2.5c, tweede, derde, vijfde en zesde lid, niet, onvolledig of niet juist heeft verstrekt en de verlener van vertrouwensdiensten niet binnen de door Onze Minister gestelde termijn de volledige of juiste gegevens alsnog verstrekt.

2. Indien de gekwalificeerde verlener van vertrouwensdiensten aantoont redelijkerwijs niet binnen de gestelde termijn, bedoeld in het eerste lid, onder b, alsnog de juiste gegevens, bedoeld in dat onderdeel, te kunnen verstrekken, kan Onze Minister de termijn verlengen.

Artikel 2.5e

Onze Minister is verantwoordelijke in de zin van artikel 1, onderdeel d, van de Wet bescherming persoonsgegevens voor een gegevensverzameling die het gevolg is van de toepassing van artikel 2.5b en voor de vertrouwenslijst, bedoeld in artikel 2.5c, eerste lid.

G

In artikel 11.5b wordt in het eerste lid ‘certificatiedienstverleners die certificaten aan het publiek afgeven,’ vervangen door ‘verleners van vertrouwensdiensten’ en wordt ‘voor de afgifte en het beheer van het certificaat is vereist’ vervangen door: voor het verlenen van de vertrouwensdienst is vereist.

H

Na artikel 11.5b wordt een artikel ingevoegd, luidende:



Artikel 11.5c

Het College bescherming persoonsgegevens is de gegevensbeschermingsautoriteit, bedoeld in artikel 19, tweede lid, van de eidas-verordening.

I

Artikel 15.1 wordt als volgt gewijzigd:

a. In de aanhef van het eerste lid wordt 'bij of krachtens deze wet' vervangen door: bij of krachtens deze wet en de eidas-verordening.

b. In het eerste lid wordt onder verlettering van onderdeel k tot onderdeel l een onderdeel ingevoegd, luidende:

k. het verlenen van vertrouwensdiensten door in Nederland gevestigde verleners van vertrouwensdiensten als geregeld in hoofdstuk III van de eidas-verordening, met inbegrip van de bijlagen waarnaar in dat hoofdstuk wordt verwezen, en de artikelen 18.15a, voor zover het Onze Minister aangaat, 18.15b tot en met 18.15e, en 18.18 van deze wet;

c. Het derde lid komt te luiden:

3. De bij besluit van het College bescherming persoonsgegevens aangewezen ambtenaren zijn belast met het toezicht op de naleving van het bepaalde bij of krachtens de artikelen 11.3a en 11.5b en, voor zover het een inbreuk op de veiligheid of het verlies van integriteit van persoonsgegevens betreft, het bepaalde bij en krachtens artikel 18.15a van deze wet en artikel 19, tweede lid van de eidas-verordening.

J

Na artikel 15.3a worden drie nieuwe artikelen ingevoegd, luidende:

Artikel 15.3b

1. De ambtenaren die door Onze Minister zijn belast met het toezicht op het verlenen van vertrouwensdiensten, zijn tevens belast met het verlenen van bijstand als bedoeld in de eidas-verordening aan een toezichthoudend orgaan uit een andere lidstaat van de Europese Unie.

2. De ambtenaren, bedoeld in het eerste lid, kunnen ten behoeve van het verlenen van bijstand hun toezichthoudende bevoegdheden toepassen, met uitzondering van de bevoegdheden, bedoeld in artikel 5:19 van de Algemene wet bestuursrecht. Artikel 15.7 van deze wet is van overeenkomstige toepassing.

3. Terzake van overtreding van artikel 5:20, van de Algemene wet bestuursrecht, zijn de artikelen 15.4, eerste lid, 15.12 en 15.14 van deze wet van overeenkomstige toepassing.

Artikel 15.3c

1. Een gemotiveerd verzoek van een toezichthoudend orgaan uit een andere lidstaat van de Europese Unie tot het verkrijgen van bijstand als bedoeld in de eidas-verordening, wijst Onze Minister op grond van artikel 18, tweede lid, onderdeel a, van de eidas-verordening in ieder geval af, indien dit verzoek strekt tot het verkrijgen van gegevens of inlichtingen waarvan de geheimhouding na verstrekking daarvan naar het oordeel van Onze Minister in onvoldoende mate zal worden gewaarborgd, voor zover sprake kan zijn van bedrijfsvertrouwelijke gegevens of inlichtingen.

2. Indien Onze Minister van oordeel is dat er sprake is van bedrijfsvertrouwelijke gegevens of inlichtingen, vermeldt Onze Minister bij het verstrekken van die gegevens of inlichtingen aan het toezichthoudend orgaan uit de andere lidstaat, uitdrukkelijk en met redenen omkleed dat die informatie niet aan derden ter beschikking mag worden gesteld.

3. Indien Onze Minister gegevens of inlichtingen verstrekt die Onze Minister heeft verkregen van een verlener van een vertrouwensdienst of een aanbieder van een gekwalificeerd middel voor het aanmaken van elektronische handtekeningen of van elektronische zegels, stelt Onze Minister de betreffende verlener of aanbieder daarvan op de hoogte.

Artikel 15.3d

1. De ambtenaren die op grond van deze wet zijn belast met het verlenen van bijstand als bedoeld in de eidas-verordening zijn bevoegd samen met een toezichthoudend orgaan uit een andere lidstaat van de Europese Unie een onderzoek uit te voeren naar de naleving van de voorschriften van die verordening, indien over dat onderzoek tussen Onze Minister en een toezichthoudend orgaan uit een andere lidstaat van de Europese Unie overeenstemming bestaat.

2. Onze Minister betrekt bij het streven naar overeenstemming in ieder geval het bepaalde in artikel 15.3c, eerste lid, omtrent geheimhouding.

3. De ambtenaren, bedoeld in het eerste lid, beschikken voor de uitvoering van een gezamenlijk onderzoek over de bevoegdheden waarover zij ook voor het verlenen van bijstand beschikken. Artikel 15.3b, derde lid, is van overeenkomstige toepassing.

4. Een persoon die voor een toezichthoudend orgaan uit een andere lidstaat aan een gezamenlijk onderzoek deelneemt, is bevoegd kennis te nemen van gegevens en inlichtingen die tijdens de uitvoering van dat onderzoek worden verkregen onder de voorwaarden van overeenstemming, bedoeld in het tweede lid.

K

Artikel 16.1, eerste lid, wordt als volgt gewijzigd:

a. In het eerste lid wordt na ‘ingevolge het bepaalde bij of krachtens deze wet’ ingevoegd: of de eidas-verordening.

b. In het tweede lid wordt na ‘naleving van het bepaalde bij of krachtens deze wet’ ingevoegd: of van de eidas-verordening.

L

Artikel 18.2a wordt als volgt gewijzigd:

a. Voor de tekst wordt de aanduiding ‘1.’ geplaatst.

b. Er worden twee leden toegevoegd, luidende:

2. Onze Minister is voor Nederland het toezichthoudend orgaan, bedoeld in artikel 17, eerste lid, van de eidas-verordening.

3. Onze Minister van Veiligheid en Justitie is het bevoegde nationale orgaan voor informatieveiligheid, bedoeld in artikel 19, tweede lid, van de eidas-verordening.

M

In artikel 18.3 worden na het derde lid drie leden toegevoegd, luidende:

4. Onze Minister, Onze Minister van Veiligheid en Justitie en het College bescherming persoonsgegevens maken in het belang van effectieve en efficiënte meldingen als bedoeld in artikel 19, tweede lid, van de eidas-verordening, afspraken over de wijze van behandeling van aangelegenheden van wederzijds belang.

5. Onze Minister en het College bescherming persoonsgegevens, maken in het belang van een effectief en efficiënt toezicht op verleners van vertrouwensdiensten die persoonsgegevens verwerken bij het verlenen van vertrouwensdiensten, afspraken over de wijze van behandeling van aangelegenheden van wederzijds belang.

6. De afspraken, bedoeld in het vierde en vijfde lid, worden in een samenwerkingsprotocol vastgelegd. Het samenwerkingsprotocol wordt bekendgemaakt in de Staatscourant.

N

In artikel 18.3a wordt na ‘op de naleving van deze wet’ ingevoegd: of van de eidas-verordening.



O

In artikel 18.7, eerste lid, wordt na ‘het bepaalde bij of krachtens deze wet’ ingevoegd: of de eidas-verordening.

P

Artikel 18.15 komt te luiden:

Artikel 18.15

Indien dit voor een goede uitvoering van de eidas-verordening vereist is, worden bij of krachtens algemene maatregel van bestuur nadere regels gegeven met betrekking tot:

a. de in deze verordening gestelde eisen aan verleners van vertrouwensdiensten en door hen te verlenen vertrouwensdiensten, waaraan een verlener van vertrouwensdiensten die aan die nadere regels voldoet het vermoeden kan ontlenen dat aan die eisen is voldaan;
b. de in deze verordening gestelde eisen aan aanbieders van gekwalificeerde middelen voor het aanmaken van elektronische handtekeningen of elektronische zegels, waaraan een aanbieder daarvan die aan die nadere regels voldoet het vermoeden kan ontlenen dat aan die eisen is voldaan.

Q

Na artikel 18.15 worden vijf artikelen ingevoegd, luidende:

Artikel 18.15a

1. Indien dit voor een goede uitvoering van de eidas-verordening vereist is, worden bij algemene maatregel van bestuur regels gesteld over de door een verlener van vertrouwensdiensten aan Onze Minister, aan Onze Minister van Veiligheid en Justitie en, voor zover het persoonsgegevens betreft, aan het College Bescherming Persoonsgegevens, te verstrekken gegevens bij de kennisgeving van een inbreuk op de veiligheid of het verlies van integriteit, bedoeld in artikel 19, tweede lid, van de eidas-verordening, en over de wijze van verstrekking van die gegevens.

2. Het eerste lid is van overeenkomstige toepassing op de kennisgeving van een inbreuk op de veiligheid of het verlies van integriteit, bedoeld in artikel 19, tweede lid, van de eidas-verordening aan degene aan wie een vertrouwensdienst is verleend die naar verwachting ongunstige gevolgen zal ondervinden van die inbreuk of dat verlies van integriteit.

Artikel 18.15b

1. Dit artikel is van toepassing op de gekwalificeerde verlener van vertrouwensdiensten die met toepassing van artikel 24, eerste lid, onderdeel a, van de eidas-verordening, een gekwalificeerd certificaat afgeeft.

2. De gekwalificeerde verlener van vertrouwensdiensten die tot afgifte van een op naam van een natuurlijk persoon gesteld gekwalificeerd certificaat overgaat, stelt daaraan voorafgaand de identiteit van die natuurlijke persoon vast aan de hand van de bij artikel 1 van de Wet op de identificatieplicht aangewezen geldige documenten.

3. De gekwalificeerde verlener van vertrouwensdiensten die tot afgifte van een op naam van een rechtspersoon gesteld gekwalificeerd certificaat overgaat, stelt daaraan voorafgaand vast:
   a. de identiteit van de natuurlijke persoon die deze rechtspersoon vertegenwoordigt aan de hand van een document als bedoeld in het tweede lid;
   b. de identiteit van de rechtspersoon door middel van raadpleging langs elektronische weg van het handelsregister, bedoeld in de Handelsregisterwet 2007, of blijkend uit een recent uittreksel uit dat register;
   c. de bevoegdheid van de natuurlijke persoon tot vertegenwoordiging van die rechtspersoon op de wijze, bedoeld in onderdeel b, of aan de hand van een volmacht, indien die volmacht is ondertekend met een gekwalificeerde elektronische handtekening als bedoeld in artikel 3, onder 12, van de eidas-verordening of een door een notaris gelegaliseerde handtekening van een natuurlijk persoon van wie de bevoegdheid tot vertegenwoordiging wordt vastgesteld op de wijze, bedoeld in onderdeel b.

4. Indien de rechtspersoon op naam van wie het gekwalificeerd certificaat wordt gesteld, wordt vertegenwoordigd door een andere rechtspersoon die door een natuurlijke persoon wordt

vertegenwoordigd of door een andere rechtspersoon die de laatste is in een reeks van elkaar aansluitend vertegenwoordigende rechtspersonen van wie de eerste door een natuurlijke persoon wordt vertegenwoordigd, wordt de identiteit van de natuurlijke persoon en zijn bevoegdheid tot vertegenwoordiging op de wijze, bedoeld in het derde lid, onderdelen a en c, vastgesteld en de identiteit van de rechtspersonen en hun bevoegdheid tot vertegenwoordiging op de wijze, bedoeld in het derde lid, onderdeel b.

5. Het vierde lid is van overeenkomstige toepassing op de natuurlijke persoon die niet een rechtspersoon maar een als zelfstandige eenheid naar buiten optredend samenwerkingsverband zonder rechtspersoonlijkheid vertegenwoordigt dat zelf weer een rechtspersoon vertegenwoordigt.

6. Indien een rechtspersoon of een samenwerkingsverband als bedoeld in het vijfde lid, niet in het handelsregister, bedoeld in de Handelsregisterwet 2007, staat ingeschreven, maar in een soortgelijk buitenlands register, wordt bij de toepassing van het derde of vierde lid, met het handelsregister dat buitenlands register bedoeld.

Artikel 18.15c

1. De gekwalificeerde verlener van vertrouwensdiensten kan met toepassing van artikel 24, eerste lid, onderdeel b, van de eidas-verordening, tot afgifte van een op naam van een natuurlijke persoon of rechtspersoon gesteld gekwalificeerd certificaat overgaan, indien een elektronisch identificatiemiddel met het betrouwbaarheidsniveau substantieel of hoog als bedoeld in dat onderdeel is afgegeven overeenkomstig de aan identificatie of vertegenwoordiging gestelde eisen, bedoeld in artikel 18.15b.

2. De gekwalificeerde verlener van vertrouwensdiensten kan met toepassing van artikel 24, eerste lid, onderdeel c, van de eidas-verordening, tot afgifte van een op naam van een natuurlijk persoon of rechtspersoon gesteld gekwalificeerd certificaat overgaan, indien een eerder afgegeven certificaat voor een gekwalificeerde elektronische handtekening of een certificaat voor een gekwalificeerd elektronisch zegel als bedoeld in dat onderdeel is afgegeven:
   a. met inachtneming van het in artikel 18.15b bepaalde;
   b. op basis van een verificatie aan de hand van een elektronisch identificatiemiddel als bedoeld in het eerste lid, dat is uitgegeven overeenkomstig het in artikel 18.15b bepaalde.

Artikel 18.15d

Indien in een gekwalificeerd certificaat andere specifieke gegevens dan die bedoeld in bijlage I, III en IV van de eidas-verordening worden vermeld, draagt de gekwalificeerde verlener van vertrouwensdiensten er zorg voor dat de juistheid van die gegevens voorafgaand aan de uitgifte van het certificaat wordt vastgesteld op een niveau dat past bij de betrouwbaarheid die aan de status gekwalificeerd wordt toegekend.

Artikel 18.15e

Voorafgaand aan de afgifte van een gekwalificeerd certificaat voor een elektronische handtekening of voor website-authenticatie waarin een natuurlijke persoon met een pseudoniem wordt aangeduid, wordt de identiteit van die natuurlijke persoon op dezelfde wijze vastgesteld als bij de afgifte van een op naam van een natuurlijke persoon gesteld gekwalificeerd certificaat.

R

De artikelen 18.16 en 18.16a vervallen.

S

In artikel 18.17 wordt ‘Degene die een veilig middel voor het aanmaken van elektronische handtekeningen op de markt brengt, zorgt er voor dat het veilig middel voldoet aan de bij of krachtens algemene bestuur te stellen eisen en, ten bewijze daarvan, dat het veilig middel is voor voorzien van’ vervangen door: Degene die een gekwalificeerd middel voor het aanmaken van elektronische handtekeningen of van elektronische zegels op de markt brengt, draagt ten bewijze dat is voldaan aan de daaraan in de eidas-verordening gestelde eisen zorg, dat het gekwalificeerd middel is voorzien van.

T

Artikel 18.17a wordt als volgt gewijzigd:



a. In het eerste lid wordt ‘veilig middel voor het aanmaken van elektronische handtekeningen’ vervangen door ‘gekwalificeerd middel voor het aanmaken van elektronische handtekeningen of elektronische zegels’ en wordt ‘artikel 18.17’ vervangen door: bijlage II van de eidas-verordening.

b. In het tweede lid, onder b, wordt na ‘om voor een aanwijzing in aanmerking te komen’ toegevoegd:, voor zover niet in die eisen door de eidas-verordening is voorzien.

c. Na het vijfde lid worden twee leden toegevoegd, luidende:

6. Een aangewezen instelling informeert Onze Minister over een gebleken overeenstemming als bedoeld in het eerste lid uiterlijk binnen twee weken na afronding van de beoordeling daarvan.

7. Bij of krachtens algemene maatregel van bestuur kunnen ter uitvoering van het zesde lid regels worden gesteld over de door een aangewezen instelling aan Onze Minister te verstrekken gegevens en over de wijze van verstrekking daarvan.

U

Artikel 18.18 komt te luiden:

Artikel 18.18

1. Het is een verlener van vertrouwensdiensten verboden in strijd te handelen met hoofdstuk III, met inbegrip van de bijlagen waarnaar in dat hoofdstuk wordt verwezen, van de eidas-verordening.

2. Het is een verlener van vertrouwensdiensten verboden zich kenbaar te maken als verlener van gekwalificeerde vertrouwensdiensten en vertrouwensdiensten als gekwalificeerd te verlenen zonder dat de status gekwalificeerd aan de verlener en de door hem te verlenen vertrouwensdiensten is toegekend en in de vertrouwenslijst is vastgelegd.

V

Aan artikel 18.22 wordt een lid toegevoegd, luidende:

3. Onze Minister doet in de Staatscourant mededeling van de titel, de vindplaats en de datum van inwerkingtreding van de eidas-verordening, alsmede van wijzigingen daarvan.

W

Na artikel 20.15 wordt een artikel ingevoegd, luidende:

Artikel 20.15a

1. Dit artikel is van toepassing op aanvragen, samenwerkingsprotocollen, archiefbescheiden en registergegevens, die tot onderwerp hebben certificatiedienstverleners of gekwalificeerde certificaten als bedoeld in artikel 1.1 van de Telecommunicatiewet, zoals die wet luidde direct voorafgaand aan de inwerkingtreding van artikel I van de Wet van .... tot wijziging van de Telecommunicatiewet, de Boeken 3 en 6 van het Burgerlijk Wetboek, de Algemene wet bestuursrecht, alsmede daarmee samenhangende wijzigingen van andere wetten in verband met de uitvoering van EU-verordening elektronische identiteiten en vertrouwensdiensten (uitvoering EU-verordening elektronische identiteiten en vertrouwensdiensten) (Stb. ....., ...).

2. Aanvragen ingediend bij de Autoriteit Consument en Markt, waarop nog geen besluit is genomen op het tijdstip van inwerkingtreding van artikel I van de wet, aangehaald in het eerste lid, worden vanaf het tijdstip van inwerkingtreding aangemerkt als aanvragen, ingediend bij Onze Minister.

3. In samenwerkingsprotocollen treedt op het tijdstip van inwerkingtreding van artikel I van de wet, aangehaald in het eerste lid, Onze Minister in de plaats van de Autoriteit Consument en Markt.

4. Archiefbescheiden van de Autoriteit Consument en Markt en aanvragen als bedoeld in het tweede lid, worden overgedragen aan Onze Minister, voor zover zij niet overeenkomstig de Archiefwet 1995 zijn overgebracht naar een archiefbewaarplaats.



5. Gegevens in het register, bedoeld in artikel 2.3, eerste lid, van de Telecommunicatiewet, zoals die luidde voorafgaand aan de inwerkingtreding van artikel I van de wet, aangehaald in het eerste lid, worden overgedragen aan Onze Minister.

X

Artikel 20.16 vervalt.

Y

Artikel 20.15a (huidig) wordt vernummerd tot artikel 20.16a.

ARTIKEL II

Boek 3 van het Burgerlijk Wetboek wordt als volgt gewijzigd:

A

Artikel 15a komt te luiden:

Artikel 15a

Evenals een elektronische gekwalificeerde handtekening als bedoeld in artikel 3, onderdeel 12, van verordening (EU) nr. 910/2014 van het Europees parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronisch transacties in de interne markt en tot intrekking van richtlijn 1999/93/EG (PbEU 2014, L 257) hebben een geavanceerde elektronische handtekening als bedoeld in onderdeel 11, en een andere elektronische handtekening als bedoeld in onderdeel 10, van artikel 3 van deze verordening dezelfde rechtsgevolgen als een handgeschreven handtekening, indien voor deze beide elektronische handtekeningen de methode voor ondertekening die gebruikt is voldoende betrouwbaar is, gelet op het doel waarvoor de elektronische handtekening is gebruikt en op alle overige omstandigheden van het geval.

B

Artikel 15b vervalt.

C

In artikel 15c wordt de zinsnede ‘vinden de bepalingen van deze afdeling’ vervangen door: vindt artikel 15a.

ARTIKEL III

Artikel 196b van Boek 6 van het Burgerlijk Wetboek vervalt.

ARTIKEL IV

Boek 7 van het Burgerlijk Wetboek wordt als volgt gewijzigd:

A

In artikel 655, derde lid, van Boek 7 van het Burgerlijk Wetboek wordt de zinsnede ‘een elektronische handtekening die voldoet aan de eisen, bedoeld in artikel 15a lid 2 van Boek 3’ vervangen door: een gekwalificeerde handtekening als bedoeld in artikel 3, onderdeel 12, van verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van richtlijn 1999/93/EG (PbEU 2014, L 257).

B

In artikel 932, eerste lid, wordt de zinsnede ‘een elektronische handtekening die voldoet aan de eisen, bedoeld in artikel 15a lid 2 van Boek 3 van het Burgerlijk Wetboek’ vervangen door: een elektronische handtekening als bedoeld in artikel 3, onderdeel 12, van verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van richtlijn 1999/93/EG (PbEU 2014, L 257)



ARTIKEL V

Artikel 2:16 van de Algemene wet bestuursrecht komt te luiden:

Artikel 2:16

1. Aan het vereiste van ondertekening is voldaan door een elektronische handtekening, indien de methode die daarbij voor ondertekening is gebruikt, voldoende betrouwbaar is, gelet op de aard en inhoud van het elektronische bericht en het doel waarvoor het is gebruikt.

2. Indien de veiligheid en de betrouwbaarheid van het elektronische bericht en het doel waarvoor het wordt gebruikt dit noodzakelijk maken, kan bij wettelijk voorschrift het gebruik worden voorgeschreven van een bepaald type elektronische handtekening als bedoeld in artikel 3, onderdeel 10, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 (PbEU 2014, L257). Daarbij kunnen aanvullende eisen worden gesteld, tenzij het gaat om een geavanceerde elektronische handtekening als bedoeld in artikel 3, onderdeel 11 of een gekwalificeerde elektronische handtekening als bedoeld in artikel 3, onderdeel 12 van die verordening.

ARTIKEL VI

In artikel 1072b, derde lid, van het Wetboek van Burgerlijke Rechtsvordering wordt de zinsnede 'een elektronische handtekening die voldoet aan het bepaalde in artikel 15a, eerste en tweede lid, van Boek 3 van het Burgerlijk Wetboek' vervangen door: een gekwalificeerde handtekening als bedoeld in artikel 3, onderdeel 12, van verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van richtlijn 1999/93/EG (PbEU 2014, L 257).

ARTIKEL VII

Artikel 7e van de Kadasterwet wordt als volgt gewijzigd:

1. In het eerste lid wordt de zinsnede 'wordt een elektronische handtekening gebruikt die voldoet aan de eisen, genoemd in artikel 15a, tweede lid, onderdelen a tot en met f, van Boek 3 van het Burgerlijk Wetboek' vervangen door: wordt een elektronische handtekening gebruikt als bedoeld in artikel 3, onderdeel 12, van verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van richtlijn 1999/93/EG (PbEU 2014, L 257)

2. Het derde lid vervalt.

ARTIKEL VIII

In artikel 8.2, eerste lid, van de Wet handhaving consumentenbescherming wordt de zinsnede '15a tot en met 15c' vervangen door: 15a en 15c.

ARTIKEL IX

In artikel 35b, vierde lid, onderdeel a, van de Wet op de omzetbelasting 1968, wordt de zinsnede 'een geavanceerde elektronische handtekening in de zin van artikel 2, lid 2, van Richtlijn 1999/93/EG van het Europees Parlement en de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen, welke gebaseerd is op een gekwalificeerd certificaat in de zin van artikel 2, lid 10, van Richtlijn 1999/93/EG en gecreëerd wordt met een veilig middel voor het aanmaken van handtekening en in de zin van artikel 2, leden 6 en 10, van Richtlijn 1999/93/EG' vervangen door: een gekwalificeerde handtekening als bedoeld in artikel 3, onderdeel 12, van verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van richtlijn 1999/93/EG (PbEU 2014, L 257).

ARTIKEL X

In artikel 34a van de Wet bescherming persoonsgegevens wordt onder vernummering van het tiende en elfde lid tot het elfde en twaalfde lid een lid ingevoegd, luidende:

10. Dit artikel is, met uitzondering van het zevende lid, niet van toepassing op de verantwoordelijke in zijn hoedanigheid als verlener van vertrouwensdiensten als bedoeld in verordening (EU) nr.



910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van richtlijn 1999/93/EG (PbEU 2014, L 257).

ARTIKEL XI

1. Artikel 1.1 van de Telecommunicatiewet, zoals dat luidde voor het tijdstip van inwerkingtreding van artikel I, onderdeel A, van deze wet, is van toepassing op de in de volgende leden gebruikte begrippen.

2. Indien voor het tijdstip van inwerkingtreding van artikel I van deze wet een aanvraag door een certificatiedienstverlener is ingediend tot registratie, bedoeld in artikel 2.1, vijfde lid, van de Telecommunicatiewet zoals dit artikellid luidde voor inwerkingtreding van artikel I van deze wet, en op het tijdstip van inwerkingtreding van deze wet hierop nog geen besluit is genomen door de Autoriteit Consument en Markt, wordt die aanvraag door Onze Minister behandeld als een aanvraag waarop deze wet van toepassing is.

3. Indien voor het tijdstip van inwerkingtreding van artikel I van deze wet een aanvraag door een instelling als bedoeld in artikel 18.17a, eerste lid, van de Telecommunicatiewet zoals die wet luidde voor inwerkingtreding van artikel I van deze wet, bij Onze Minister is ingediend en op het tijdstip van inwerkingtreding van deze wet hierop nog geen besluit is genomen, wordt die aanvraag door Onze Minister behandeld als een aanvraag waarop deze wet van toepassing is.

4. Ten aanzien van de behandeling van bezwaar of beroep dat voor of na het tijdstip van inwerkingtreding van deze wet is gemaakt of ingesteld tegen een besluit genomen door de Autoriteit Consument en Markt voor de inwerkingtreding van artikel I van deze wet op een aanvraag door een certificatiedienstverlener tot registratie als bedoeld in artikel 2.1, vijfde lid, van de Telecommunicatiewet zoals dit artikellid luidde voor inwerkingtreding van artikel I van deze wet, is het recht zoals dat gold voor het tijdstip van inwerkingtreding van artikel I van deze wet van toepassing en behandelt de Autoriteit Consument en Markt het gemaakte bezwaar of ingestelde beroep.

5. Ten aanzien van de behandeling van bezwaar of beroep dat voor of na het tijdstip van inwerkingtreding van deze wet is gemaakt of ingesteld tegen een besluit genomen door Onze Minister voor de inwerkingtreding van artikel I van deze wet op een aanvraag door een instelling als bedoeld in artikel 18.17a, eerste lid, van de Telecommunicatiewet zoals dit artikellid luidde voor inwerkingtreding van deze wet, is het recht zoals dat gold voor het tijdstip van inwerkingtreding van artikel I van deze wet van toepassing.

6. Een door de Minister aangewezen instelling als bedoeld in artikel 18.17a, eerste lid, van de Telecommunicatiewet zoals dit artikellid luidde voor inwerkingtreding van artikel I van deze wet, wordt na inwerkingtreding van artikel I van deze wet aangemerkt als een aangewezen instelling als bedoeld in dat artikel.

ARTIKEL XII

1. De artikelen van deze wet treden in werking op een bij koninklijk besluit te bepalen tijdstip, dat voor de verschillende artikelen of onderdelen daarvan verschillend kan worden vastgesteld.

2. In het besluit, bedoeld in het eerste lid, wordt zo nodig toepassing gegeven aan artikel 12 van de Wet raadgevend referendum bij de inwerkingtreding van artikelen of onderdelen van het voorstel van wet die zijn gewijzigd na indiening van het voorstel bij de Tweede Kamer der Staten-Generaal.

Lasten en bevelen dat deze in het Staatsblad zal worden geplaatst en dat alle ministeries, autoriteiten, colleges en ambtenaren die zulks aangaat, aan de nauwkeurige uitvoering de hand zullen houden.

De Minister van Economische Zaken,

De Minister van Veiligheid en Justitie,

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,



MEMORIE VAN TOELICHTING

Inhoudsopgave

III. Implementatietabel

I. Algemeen

1. Inleiding

Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG (PbEU 2014, L 257) (hierna verder genoemd: de verordening of de eidas-verordening) is een van de initiatieven ter uitvoering van de Digitale agenda voor Europa. Doel van de verordening is het vertrouwen in elektronische transacties te vergroten door te voorzien in een gemeenschappelijke grondslag voor veilige elektronische interactie tussen burgers, bedrijven en overheden, en bijgevolg ook de doeltreffendheid van publieke en private onlinediensten en elektronische handel in de interne markt van de Europese Unie te verhogen. De verordening regelt daartoe het grensoverschrijdend gebruik van elektronische identificatiemiddelen en vertrouwensdiensten tussen de lidstaten van de Europese Unie. De verordening is vanaf 1 juli 2016 van toepassing op vertrouwensdiensten inclusief het toezicht daarop en vanaf 18 september 2018 op de verplichte erkenning van elektronische identificatiemiddelen uit andere lidstaten. De verordening vervangt richtlijn 1999/93/EG van het Europees Parlement en de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen (PbEG 2000, L 13) (hierna: de richtlijn of de Richtlijn elektronische handtekeningen). Aan het einde van de artikelsgewijze toelichting is een omzettingstabel van de eidas-verordening opgenomen. Deze memorie van toelichting wordt uitgebracht mede namens de Minister van Veiligheid en Justitie en de Minister van Binnenlandse Zaken en Koninkrijksrelaties.

Naast feitelijke uitvoering vereist het deel van de verordening dat over vertrouwensdiensten gaat, ook wijziging van wetgeving. Daarin voorziet dit wetsvoorstel, waarbij het uitgangspunt van de rechtstreekse werking van de verordening en minimumomzetting wordt gerespecteerd. Het wetsvoorstel strekt uitsluitend tot omzetting van de eidas-verordening. Het wetsvoorstel leidt tot wijziging van de Telecommunicatiewet (hierna ook: Tw) en van enkele artikelen uit onder meer het Burgerlijk Wetboek (hierna ook: BW), de Algemene wet bestuursrecht (hierna ook: Awb) en de Wet bescherming persoonsgegevens (hierna ook: Wbp). De voorgestelde wijzigingen in de Tw zien deels op het laten vervallen van artikelen als gevolg van de rechtstreekse werking van de verordening, zoals de bepaling om bij of krachtens de Tw eisen te stellen aan certificatiedienstverleners en hun diensten. De verordening voorziet zelf voor alle EU-lidstaten in de eisen waaraan verleners van (gekwalificeerde) vertrouwensdiensten moeten voldoen. In het wetsvoorstel vervalt bijvoorbeeld ook het wettelijk geregelde vermoeden van overeenstemming (artikel 18.16a Tw). Het oordeel of al dan niet aan de eisen uit de verordening wordt voldaan is aan de toezichthouder en kan niet louter op een verslag van een conformiteitsbeoordelingsinstantie als bedoeld in de verordening worden gebaseerd. Andere voorgestelde wijzigingen leiden tot aanpassing of invoeging van voorschriften. Het wetsvoorstel regelt de samenloop tussen de meldplicht aan aangewezen (toezichthoudende) organen bij een inbreuk die de veiligheid of integriteit van vertrouwensdiensten aantast en de samenloop met in andere wetgeving voorkomende meldplichten. Een ander onderwerp dat in het wetsvoorstel aan bod komt, is toezicht en handhaving. Het wetsvoorstel wijst de Minister van Economische Zaken aan als toezichthoudend orgaan voor in Nederland gevestigde verleners van vertrouwensdiensten, en kan op grond van het wetsvoorstel ambtenaren van Agentschap Telecom (hierna ook: AT) met het toezicht belasten. Daarnaast voorziet het wetsvoorstel in de voor toezicht en handhaving benodigde bevoegdheden en in de overgang van het toezicht van de Autoriteit Consument en Markt (hierna: ACM) op gekwalificeerde certificaten voor elektronische handtekeningen naar de Minister, feitelijk AT. Over grensoverschrijdende samenwerking tussen toezichthoudende organen van EU-lidstaten stelt het wetsvoorstel bevoegdheden en voorwaarden vast voor het vanuit Nederland verlenen van bijstand of het verrichten van gezamenlijk onderzoek.

Naast voorgestelde aanpassingen in de Tw zijn er ook voorgestelde wijzigingen in de Boeken 3 en 6 van het BW. Die zien op de rechtsgevolgen die aan het gebruik van bepaalde vertrouwensdiensten worden verbonden, op de positie van verleners van vertrouwensdiensten uit derde landen, en op aansprakelijkheid van verleners van vertrouwensdiensten. Voor zover nodig, vervallen in het wetsvoorstel bepalingen hierover op grond van de rechtstreekse werking van de verordening. Ook is er een voorgestelde wijziging van de Awb, die op de elektronische handtekening betrekking heeft. Als onderdeel van het geheel aan wijzigingen dat de samenloop tussen de meldplichten voor vertrouwensdiensten en het toezicht daarop regelt, wordt tot slot een specifieke wijziging van de Wbp voorgesteld.

Het algemeen deel van deze memorie van toelichting is als volgt opgezet:
– uitleg wat elektronische identificatiemiddelen, vertrouwensdiensten en certificaten zijn in relatie tot gerechtvaardigd vertrouwen bij digitaal verkeer (paragraaf 2);

- een uiteenzetting op hoofdlijnen van de inhoud van de verordening en de gevolgen daarvan voor feitelijke uitvoering en wetgeving (paragraaf 3);
- per thema telkens een afzonderlijke uitleg van de inhoud van de verordening en een toelichting op de gevolgen daarvan voor feitelijke uitvoering en wetgeving (paragrafen 4 tot en met 8);
- een toelichting op aanpassing van overige wetgeving, overgangsrecht, samenloop, administratieve lasten, financiële gevolgen, uitvoering en handhaving en de uitkomsten van internetconsultatie op het wetsvoorstel (paragrafen 9 tot en met 13).

2. De eidas-verordening en gerechtvaardigd vertrouwen bij digitaal verkeer

2.1 Elektronische identificatie en elektronische identificatiemiddelen

Dienstverlening kan persoonlijk zijn. Een dienstaanbieder wil dan weten wie de dienst wil afnemen. In de fysieke wereld worden hier identiteitsbewijzen, zoals het paspoort, de identiteitskaart of het rijbewijs voor gebruikt. Die bevatten identificerende gegevens van een persoon zoals een voornaam, achternaam, geboortedatum, geboorteplaats, foto en mogelijk een uniek identificerend nummer, zoals in Nederland het Burgerservicenummer (BSN). Het document bevat eveneens echtheidskenmerken zoals een speciaal bewerkte foto, een zegel of hologram. Daardoor weet iemand die het identiteitsdocument controleert met wie hij te maken heeft, dat het om een echt document gaat en daardoor dat de gegevens op het document authentiek zijn.

Elektronische identificatie is digitaal en verloopt anders. Preciezer gesteld is elektronische identificatie een proces waarbij persoonsidentificatiegegevens in elektronische vorm worden gebruikt. Met die gegevens wordt een persoon uniek aangeduid. (artikel 3, onderdeel 1, van de verordening). Unieke aanduiding maakt onderscheid tussen personen mogelijk. Het voorkomt dat de ene persoon wordt verward of verwisseld met een andere. In de verordening gaat het hierbij niet enkel om elektronische identificatie van natuurlijke personen, maar ook om rechtspersonen die zijn opgericht naar of worden beheerst door het recht van een lidstaat. Elektronische identificatie in de zin van de verordening kan voorts ook betrekking hebben op natuurlijke personen die bevoegd voor deze rechtspersonen handelen, zoals op basis van wettelijke vertegenwoordiging of een volmacht. Elektronische identificatie die niet in de verordening is geregeld, is bijvoorbeeld identificatie van een natuurlijke persoon die een andere natuurlijke persoon vertegenwoordigt of identificatie van apparaten, systemen of computerprogrammatuur.

Bij elektronische identificatie kan gebruik worden gemaakt van elektronische identificatiemiddelen (artikel 3, onderdeel 2, van de verordening). De persoonsidentificatiegegevens zijn dan bijvoorbeeld opgeslagen in een chip die is geïntegreerd in een pasje of zijn aanwezig in een beveiligde omgeving binnen een informatiesysteem. De controle over het gebruik van persoonsidentificatiegegevens berust bij de persoon van wie de identiteit is. Het gebruik kan plaatsvinden met kennis die geheim blijft voor anderen, bijvoorbeeld een zelfgekozen wachtwoord of pincode. Het kan ook met een middel in combinatie met (wisselende) gegevens, bijvoorbeeld voortkomend uit een nummercalculator, token of mobiele telefoon. Tenslotte kan het gebruik van de persoonsidentificatiegegevens fysiek gebonden zijn aan biometrische kenmerken, zoals een vingerafdruk, stemherkenning of irisscan. Een combinatie van methoden leidt tot meer veiligheid en minder kans op identiteitsfraude. Bijvoorbeeld het invullen van een gebruikersnaam, wachtwoord op een website, waarna vervolgens een verificatiecode afkomstig van een nummercalculator op een telefoon moet worden ingevoerd. Dit wordt meerfactorauthenticatie genoemd. De kans dat een derde over beide geheime en persoonsgebonden factoren beschikt is kleiner dan bij gebruik van een enkelvoudige methode. Voorwaarde daarvoor is het zorgvuldig gebruik en bewaren van geheime gegevens en bijbehorende middelen.

De functie van het gebruik van elektronische identificatiemiddelen is dat een persoon elektronisch duidelijk kan maken aan een ander wie hij is en dat hij het echt is. Het is gericht op het creëren van gerechtvaardigd vertrouwen bij een ander. Dit gebeurt doordat het gebruik van een elektronisch identificatiemiddel via een elektronisch proces leidt tot een bevestiging van de echtheid van een aan een ander opgegeven of kenbaar gemaakte identiteit. Die elektronische bevestiging van echtheid die de vertrouwende partij ontvangt, is in veel situaties afkomstig van een derde partij die de identiteit op echtheid heeft gecontroleerd en vastgelegd. Het proces dat bevestiging van echtheid mogelijk maakt, heeft een specifieke naam: authenticatie (artikel 3, onderdeel 5, van de verordening).

De betrouwbaarheid van elektronische identificatiemiddelen kan verschillend zijn. Dit hangt af van de betrouwbaarheid van de keten die op het elektronisch identificatiemiddel is gericht. Bij deze keten kunnen meerdere partijen betrokken zijn. De betrouwbaarheid van het middel wordt bepaald door onder meer de koppeling tussen persoonsidentificatiegegevens met de persoon, het uitgifteproces van een elektronisch identificatiemiddel, het beheer van het middel, de gebruikte techniek en de inrichting van het authenticatieproces.

Het gebruik van een elektronisch identificatiemiddel kan in de nabijheid van een vertrouwende partij plaatsvinden. Bijvoorbeeld elektronische identificatie in onmiddellijke nabijheid om vervolgens een fysiek product in ontvangst te kunnen nemen. Het creëren van gerechtvaardigd vertrouwen is echter bij uitstek ook geschikt voor partijen die elektronisch en op afstand met elkaar in contact staan. Voor elektronische identificatiemiddelen als bedoeld in de verordening is het zelfs een voorwaarde dat die worden gebruikt voor authenticatie bij een onlinedienst, en dus elektronisch op afstand.

2.2 Vertrouwensdiensten

Onder vertrouwensdiensten worden in de verordening samengevat elektronische handtekeningen, elektronische zegels, elektronische tijdstempels, diensten voor aangetekende elektronische bezorging en elektronische certificaten voor authenticatie van websites verstaan. Deze diensten worden gewoonlijk tegen betaling verricht. Er wordt bij vertrouwensdiensten een verbinding met andere gegevens gelegd. Dit wordt associatie genoemd. Met een elektronische handtekening kan bijvoorbeeld een digitale overeenkomst worden ondertekend. Met een elektronisch zegel kan een diploma of uittreksel door een instantie elektronisch gewaarmerkt worden. Een certificaat voor de authenticatie van een website maakt een gebruiker duidelijk of een website echt is en dat hij daadwerkelijk met de bedoelde website communiceert. Vertrouwensdiensten dragen bij aan het vertrouwen in elektronisch verkeer.

De meest bekende vertrouwensdienst is de elektronische handtekening. Een elektronische handtekening bestaat uit gegevens in elektronische vorm die gehecht zijn aan of logisch verbonden zijn met andere gegevens in elektronische vorm en die door de ondertekenaar worden gebruikt om te ondertekenen (artikel 3, onderdeel 10, van de verordening). Ondertekenaar is een natuurlijke persoon die een elektronische handtekening aanmaakt (artikel 3, onderdeel 9, van de verordening). Door ondertekening drukt de ondertekenaar iets uit ten aanzien van de vastgelegde gegevens. Bijvoorbeeld: ‘ik ben de auteur van dit document’ of ‘ik heb dit document in ontvangst genomen’, of ‘ik ben akkoord met de inhoud van dit document’.

Een elektronisch zegel kan worden gebruikt door een rechtspersoon die is opgericht naar of wordt beheerst door het recht van een lidstaat van de Europese Unie. Het zegel betreft gegevens in elektronische vorm die gehecht zijn aan of logisch verbonden zijn met andere gegevens in elektronische vorm en die worden gebruikt om de oorsprong en integriteit daarvan te waarborgen (artikel 3, onderdeel 25, van de verordening). Een rechtspersoon die bijvoorbeeld elektronisch een diploma, een getuigschrift of een uittreksel uit een administratie verstrekt, kan dit van een elektronisch zegel voorzien. Daarmee wordt beoogd te waarborgen dat het elektronisch document van een bepaalde entiteit afkomstig is. De organisatie van een rechtspersoon is verantwoordelijk voor een zorgvuldig en bevoegd gebruik van een elektronisch zegel. Voor de vertrouwende partij is niet herkenbaar wie de natuurlijke persoon is die de rechtspersoon vertegenwoordigt bij het aanmaken van het zegel. Daardoor kan een vertrouwende partij de bevoegdheid tot vertegenwoordiging door de natuurlijke persoon op grond van de wet, statuten of een volmacht niet controleren. Dit is enkel anders indien aanvullende gegevens (attributen) over de identiteit van de natuurlijke persoon onderdeel zijn van het elektronisch zegel. Het voorzien van een elektronisch document van een elektronisch zegel is te onderscheiden van de ondertekening daarvan. Voor de totstandkoming van bijvoorbeeld een elektronische onderhandse akte, zoals een elektronische verzekeringspolis, is op grond van artikel 932, eerste lid, van Boek 7 van het Burgerlijk Wetboek (hierna verder: BW) ondertekening daarvan met een elektronische handtekening vereist.

Een elektronisch tijdstempel betreft gegevens in elektronische vorm die andere gegevens in elektronische vorm verbinden aan een bepaald tijdstip en die bewijzen dat die laatstgenoemde gegevens op dat tijdstip bestonden (artikel 3, drieëndertigste lid, van de verordening). Dit kan belangrijk zijn bij processen waaraan tijdslimieten zijn verbonden voor het indienen van stukken en aanvragen. Aanbestedingsprocedures, subsidieaanvragen en belastingaangiftes zijn hier voorbeelden van.

Een dienst van aangetekende elektronische bezorging verschaft bewijs over het verzenden van elektronische gegevens en de ontvangst daarvan. Daarbij zijn de verzonden gegevens beschermd tegen het risico van verlies, diefstal, beschadiging en onbevoegde wijziging (artikel 3, onderdeel 36, van de verordening). Net als aangetekende post kan de dienst van aangetekende elektronische bezorging worden gebruikt voor verzending en ontvangst van belangrijke documenten. Bij het verlenen van een dienst voor elektronisch aangetekende bezorging geldt niet als vereiste dat de geadresseerde of iemand voor hem de ontvangst van een bericht elektronisch ‘in persoon’ moet bevestigen. Een bewijs van ontvangst kan zich bij een dergelijke dienst ook beperken tot de bevestiging dat een bericht op een account is afgeleverd. Indien met een bepaalde mate van betrouwbaarheid moet worden vastgesteld of de geadresseerde daadwerkelijk kennis heeft genomen van de ontvangst van een bericht, dan hangt het van de inrichting van de dienst af of dit is gewaarborgd. Bij de zogenoemde gekwalificeerde elektronisch aangetekende bezorging wordt bijvoorbeeld de eis

gesteld dat de identiteit van de geadresseerde wordt bevestigd, alvorens de gegevens worden bezorgd.

Door gebruik van een certificaat voor authenticatie van websites weet een burger of bedrijf dat hij zich echt op de gewenste website bevindt en niet op een namaaksite (artikel 3, onderdeel 38, van de verordening). Het stelt bezoekers van een website in staat met een bepaalde mate van betrouwbaarheid vast te stellen welke persoon of organisatie achter de website zit die ze online bezoeken. Visueel wordt dit gewoonlijk zichtbaar door het tonen van een slotje, vaak in combinatie met de groene kleur van de adresbalk. Websitecertificaten worden veel gebruikt als bron van vertrouwen in websites, onder meer voor internetbankieren, overheidswebsites en webwinkels. Het gebruik daarvan is essentieel voor betrouwbare toegang tot een website.

Aanvullende vertrouwensdiensten zien op de validering en bewaring van elektronische handtekeningen en -zegels. Validering is het proces waarmee wordt nagegaan of en bevestigd dat een elektronische handtekening of zegel geldig is (artikel 3, onderdeel 41, van de verordening). Bewaringsdiensten zorgen ervoor dat ook na verloop van tijd nog kan worden vastgesteld of een indertijd gebruikte elektronische handtekening of -zegel echt en geldig was. Dit waarborgt de bewijsfunctie van bijvoorbeeld ondertekende of gewaarmerkte elektronische documenten die gearchiveerd zijn en waarbij de technologische geldigheid van de elektronische handtekening of het zegel inmiddels is verlopen. Dit vereist maatregelen die het bijvoorbeeld mogelijk maken na te gaan of de betreffende vertrouwensdienst indertijd geldig was gebruikt en of gegevens achteraf niet aangepast zijn. Elektronische overeenkomsten, zoals koopcontracten die langs digitale weg tot stand komen, zijn een voorbeeld van mogelijke toepassing van deze dienst.

Vertrouwensdiensten worden vaak gebruikt bij het verzenden en ontvangen van elektronische documenten. Onder elektronische documenten wordt elke inhoud verstaan die in elektronische vorm is opgeslagen. Hier valt tekst onder maar ook geluid, beeld en zelfs audiovisuele opnames. De verordening bepaalt dat elektronische documenten rechtsgevolgen kunnen hebben en als bewijsmiddel gebruikt kunnen worden in gerechtelijke procedures.

2.3 Certificaten onderdeel van vertrouwensdiensten

Certificaten kunnen onderdeel zijn van een vertrouwensdienst, maar ook van een elektronisch identificatiemiddel. Een certificaat is een gegevensbestand waarin onder meer identiteitsgegevens staan vermeld van degene op naam van wie het certificaat staat, de geldigheidsduur ervan en de partij die het certificaat heeft afgegeven. Voorafgaand aan de afgifte van het certificaat controleert de verstrekkende derde partij de identiteit van de persoon voor wie het certificaat bestemd is en registreert dit. Na afgifte kan de houder van het certificaat met behulp van unieke (geheime) private sleutel het certificaat gebruiken. Om deze sleutelgegevens onder zijn controle te houden, kan een middel zoals een smartcard, USB-stick, mobiele telefoon of token worden gebruikt. Een certificaat kan door de houder ervan gekoppeld worden aan door hemzelf gekozen of aangemaakte andere gegevens, bijvoorbeeld aan een elektronisch document. Hierdoor wordt de integriteit of herkomst, of eventueel ook de vertrouwelijkheid van dat document gewaarborgd. Degene die elektronisch en op afstand vertrouwt op een certificaat gekoppeld aan bijvoorbeeld een document, zal bepaalde gegevens in een certificaat moeten kunnen inzien en bevestigd krijgen dat het certificaat nog geldig en niet ingetrokken is. Daarvoor moet de vertrouwende partij beschikken over unieke publieke sleutelgegevens. Die sleutelgegevens zijn vastgelegd in het publieke deel van het certificaat of zijn bijvoorbeeld via een webbrowser toegankelijk. In de toelichting op het wetsvoorstel Wet elektronische handtekeningen is de werking van certificaten in verband met asymmetrische cryptologie toegelicht (Kamerstukken II 2000/01, 27 743, nr. 3, blz. 2 en 3).

In de verordening worden specifieke eisen gesteld aan het verlenen van gekwalificeerde certificaten voor elektronische handtekeningen, voor elektronische zegels en voor website-authenticatie (artikel 3, vijftiende lid, dertigste lid en achtendertigste lid). Door aan deze certificaten specifieke eisen te stellen en door het toezicht daarop verhoogt dit de betrouwbaarheid van die certificaten. Een eis die bij de afgifte van een dergelijk gekwalificeerd certificaat van toepassing is, is dat verificatie van de identiteit in fysieke aanwezigheid moet plaatsvinden. Anders dan onder de richtlijn geldt dit alleen bij de eerste afgifte en kan verificatie bij een vervolgverzoek onder voorwaarden online en op afstand plaatsvinden. Daarmee worden de mogelijkheden voor het op afstand verkrijgen van een gekwalificeerd certificaat in de praktijk vereenvoudigd.

3. De inhoud en gevolgen van de eidas-verordening op hoofdlijnen

3.1 Inhoud eidas-verordening op hoofdlijnen

Indien een lidstaat van de Europese Unie de onlinetoegang tot publieke diensten afhankelijk stelt van

een elektronisch identificatiemiddel dat nationaal is uitgegeven, belemmert dit de toegang tot die onlinedienst voor burgers of bedrijven uit andere lidstaten. Bijvoorbeeld de toegang tot een onlineportal of persoonlijke omgeving om bepaalde administratieve processen af te kunnen wikkelen. Om hierin verandering te brengen bevat de verordening een verplichte erkenning van elektronische identificatiemiddelen uit andere lidstaten waarvan het onderliggende stelsel is aangemeld bij de Europese Commissie. Met aangemelde elektronische identificatiemiddelen kunnen burgers en bedrijven zich ook toegang verschaffen tot onlinediensten die door openbare instanties uit andere lidstaten onder de in nationale wetgeving gestelde voorwaarden worden aangeboden en waarvoor het gebruik van een elektronisch identificatiemiddel vereist is. Deze verplichte erkenning door openbare instanties van aangemelde elektronische identificatiemiddelen beperkt zich tot die middelen, die het betrouwbaarheidsniveau substantieel of hoog hebben. Een openbare instantie hoeft geen elektronisch identificatiemiddel te erkennen dat een lager betrouwbaarheidsniveau heeft dan voor de onlinedienst vereist is. Voorbeelden waarbij erkenning aan de orde kan zijn, is het met behulp van een aangemeld elektronisch identificatiemiddel in een andere lidstaat doen van online belastingaangifte of het realiseren van een elektronische inschrijving bij een universiteit. Een lidstaat is niet verplicht tot het aanmelden van een stelsel bij de Europese Commissie over te gaan om erkenning te bewerkstelligen. De verordening preciseert de verantwoordelijkheid van een lidstaat voor onderdelen van een aangemeld stelsel en de aansprakelijkheid die daarbij geldt.

De verordening is tevens van toepassing op vertrouwensdiensten die samengevat aan het publiek worden aangeboden (zie hiervoor verder de toelichting bij artikel I, onderdeel F, artikel 2.5a). Uitgangspunt in de verordening is dat de verlener van vertrouwensdiensten gevestigd in de ene lidstaat niet wordt belemmerd in het verlenen van zijn diensten in een andere lidstaat. In de verordening wordt verder onderkend dat betrouwbaar elektronisch verkeer wezenlijk is. De verordening regelt de eisen waaraan moet worden voldaan bij het verlenen van vertrouwensdiensten aan het publiek en waaraan het toezicht hierop moet voldoen. De verordening maakt hierbij onderscheid tussen het verlenen van niet-gekwalificeerde en gekwalificeerde vertrouwensdiensten. De functie van de dienst is steeds dezelfde. Het verschil is dat aan het verlenen van gekwalificeerde vertrouwensdiensten en de verleners daarvan specifieke eisen worden gesteld en het toezicht daarop specifieker en verdergaand is geregeld. Iedere verlener van vertrouwensdiensten aan het publiek is gehouden tot het treffen van passende organisatorische en technische veiligheidsmaatregelen. De lidstaten dienen te voorzien in een beperkte vorm van toezicht achteraf op de naleving hiervan bij niet-gekwalificeerde vertrouwensdiensten. Verder dient iedere verlener van vertrouwensdiensten te voldoen aan informatieverplichtingen, indien sprake is van een veiligheidsinbreuk of integriteitsverlies met aanzienlijke gevolgen voor de vertrouwensdienst. Voorts regelt de verordening dat gekwalificeerde vertrouwensdiensten niet eerder als zodanig mogen worden aangeboden, dan nadat daarvoor de status gekwalificeerd is toegekend door het door een lidstaat aangewezen toezichthoudend orgaan. Het toezichthoudend orgaan dient in de verordening vastgestelde taken te vervullen, waaronder die ten aanzien van de uitoefening van toezicht op verleners van vertrouwensdiensten en hun diensten, het delen van gegevens met andere toezichthouders, het verlenen van bijstand, samenwerking met toezichthoudende organen uit andere lidstaten van de Europese Unie en het opstellen en bijhouden van vertrouwenslijsten. De mogelijkheid van vrijwillige accreditatie, die de richtlijn bood, komt niet terug in de verordening. Ook certificaten voor de authenticatie van websites worden gerekend tot vertrouwensdiensten. Die zijn, zoals uit het incident DigiNotar najaar 2011, is gebleken voor het realiseren van digitale betrouwbaarheid bij onlineverkeer essentieel.

Er kunnen met behulp van vertrouwensdiensten rechtshandelingen tot stand komen en de bewijsvoering kan ermee worden vergemakkelijkt. De verordening bevat regels die gaan over de rechtsgevolgen die aan het gebruik van vertrouwensdiensten zijn verbonden en over het gebruik van vertrouwensdiensten als bewijs in gerechtelijke procedures. Daarnaast is de grensoverschrijdende erkenning van bepaalde elektronische handtekeningen/zegels door openbare instanties die onlinediensten aanbieden onderwerp van de verordening, evenals de positie van verleners van vertrouwensdiensten uit derde landen en aansprakelijkheid.

De verordening doet geen afbreuk aan nationaal of Unierecht dat betrekking heeft op de totstandkoming en geldigheid van contracten of andere wettelijke of procedurele verplichtingen inzake vormvereisten. Een toegestaan vormvereiste, is het vereiste dat een door de notaris opgemaakt authentieke akte op (bepaald) papier gesteld dient te zijn. De voorschriften over vertrouwensdiensten in de verordening respecteren dit.

3.2 Voorgestelde uitvoering eidas-verordening op hoofdlijnen

Een EU-verordening werkt rechtstreeks en lidstaten van de Europese Unie zijn verplicht om alle maatregelen te nemen die nodig zijn voor de volledige verwezenlijking van een verordening. Gelet op het rechtstreekse karakter, maakt een verordening automatisch deel uit van de nationale rechtsorde en is het verboden om bepalingen ervan in het nationale recht over te nemen. Voorkomen moet worden

dat een nationale regeling opnieuw datgene bepaalt dat reeds in een rechtstreeks toepasselijke verordening wordt bepaald. Daartoe moeten de met de desbetreffende verordening strijdige bepalingen uit het nationale recht als ook de bepalingen uit de nationale regeling die hetzelfde regelen als de verordening worden geschrapt (arrest van het Hof van Justitie van de Europese Gemeenschap van 7 februari 1973, zaak C-39/72, ECLI:EU:C:1973:13). Wel kan het voor de operationalisering van een verordening nodig zijn om bepalingen met betrekking tot handhaving, rechtsbescherming en aanwijzing van uitvoeringsorganen op te nemen in nationale regelgeving. Daarnaast kan het noodzakelijk zijn feitelijke maatregelen te treffen. De eidas-verordening maakt zowel feitelijke uitvoeringswerkzaamheden als aanpassing van regelgeving noodzakelijk. Het deel van de eidas-verordening over elektronische identificatie vereist enkel feitelijke uitvoering. Hierbij vervult de ontwikkeling van een landelijk knooppunt dat grensoverschrijdende elektronische identificatie mogelijk maakt een belangrijke rol (zie verder paragraaf 4 van deze toelichting). Voor het deel van de verordening dat over vertrouwensdiensten gaat, is naast feitelijke uitvoering ook wijziging van regelgeving voorgesteld.

Die voorgestelde wijzigingen zien niet op ieder voorschrift over vertrouwensdiensten uit de verordening, zoals de voor iedere verlener van vertrouwensdiensten geldende verplichting tot het treffen van passende veiligheidsmaatregelen (zie verder de paragrafen 5.1 en 5.2 van deze toelichting). Een verplichting die wel tot een voorgestelde wetswijziging leidt, betreft de meldplichten bij een veiligheidsinbreuk. Het wetsvoorstel voorziet in het aanwijzen van (toezichthoudende) organen waaraan een veiligheidsinbreuk op vertrouwensdiensten gemeld moet worden en op de samenwerking tussen hen. Ook de samenloop met in andere wetgeving voorkomende meldplichten wordt in het wetsvoorstel geregeld (zie verder de paragrafen 5.3 en 5.4 van deze toelichting). Te onderscheiden van voorschriften in de verordening waaraan iedere verlener van vertrouwensdiensten moet voldoen, zijn voorschriften in de verordening die uitsluitend en specifiek relevant zijn voor verleners van gekwalificeerde vertrouwensdiensten. Dit leidt tot diverse voorgestelde wijzigingen van de Tw. Allereerst betreft dit het laten vervallen van bestaande wetsartikelen, zoals de bepaling dat bij of krachtens de Tw eisen worden gesteld aan certificatiedienstverleners en hun diensten. Die eisen regelt de verordening zelf door in een groot aantal artikelen specifieke eisen aan verleners van gekwalificeerde vertrouwensdiensten en hun gekwalificeerde vertrouwensdiensten te stellen. Andere voorbeelden van voorgestelde wijzigingen zijn het vervallen van de bepaling die de aanwijzing door de Minister van Economische Zaken van certificeringsinstellingen regelt die door certificatiedienstverleners kunnen worden ingeschakeld en over het wettelijk geregelde vermoeden van overeenstemming (artikelen 18.16 en 18.16a, van de Tw). Voorgestelde aanpassingen strekken niet enkel tot het vervallen van bepalingen uit de Tw, maar richten zich ook op nieuwe of aanvullende bepalingen in de Tw ter uitvoering van de verordening. Het wetsvoorstel voorziet bijvoorbeeld bij de afgifte van gekwalificeerde certificaten aan natuurlijke personen en rechtspersonen in de wijze van vaststelling van de identiteit en vertegenwoordigingsbevoegdheid. De verordening laat die vaststelling uitdrukkelijk bij de EU-lidstaten zelf. Ook bevat het wetsvoorstel de mogelijkheid om bij algemene maatregel van bestuur technische normen aan te wijzen, voor zover de Europese Commissie daarin niet heeft voorzien en dit voor een goede uitvoering van de verordening nodig is. Evenals in de verordening levert het voldoen aan die normen een rechtsvermoeden voor de verlener van vertrouwensdiensten op dat aan de daarop betrekking hebbende bovenliggende eisen in de verordening is voldaan. Tot slot wordt de Minister van Economische Zaken in het wetsvoorstel aangewezen als orgaan dat de vertrouwenslijst voor gekwalificeerde vertrouwensdiensten opstelt en bijhoudt (zie verder de paragrafen 5.5 en 5.6 van deze toelichting).

Over toezicht, handhaving en grensoverschrijdende samenwerking tussen toezichthouders worden eveneens wijzigingen van de Tw voorgesteld. Het wetsvoorstel wijst de Minister van Economische Zaken, die verantwoordelijk is voor het dienstonderdeel Agentschap Telecom (hierna verder ook: AT), als toezichthoudend orgaan aan. Het wetsvoorstel regelt dat de Minister ambtenaren van AT met het toezicht op verleners van vertrouwensdiensten kan belasten. Het wetsvoorstel regelt daarbij de overgang van het toezicht van ACM op gekwalificeerde certificaten voor elektronische handtekeningen naar de Minister, feitelijk AT (zie verder de paragrafen 5.7 en 5.8 van deze toelichting).

Voorgestelde wijzigingen in andere wetten hebben verder betrekking op de artikelen 3:15 a tot met c en artikel 6:196b, van het BW, artikel 2.16 van de Awb, en artikelen in verscheidene andere wetten die onder meer verwijzen naar artikelen met begrippen die door de rechtstreekse werking van de verordening worden vervangen. De voorgestelde veranderingen in Boek 3 respectievelijk Boek 6 van het BW zien op het vervallen van bestaande bepalingen over aansprakelijkheid van certificatieverleners (zie verder de paragrafen 5.9 en 5.10 van deze toelichting) en over certificatiedienstverleners uit derde landen (zie verder de paragrafen 5.11 en 5.12 van deze toelichting). De verordening voorziet daarin met rechtstreekse werking, waardoor genoemde bepalingen overbodig worden. De overige voorgestelde wijzigingen in Boek 3 van het BW en in de Awb hangen samen met de rechtsgevolgen verbonden aan het gebruik van de elektronische handtekening (zie verder de paragrafen 6.1 en 6.2 van deze toelichting). Voor zover in andere wetgeving naar de desbetreffende bepalingen uit deze wetten wordt verwezen, voorziet dit wetsvoorstel tevens in aanpassing daarvan.

De voorschriften in de verordening over de erkenning van vertrouwensdiensten door openbare instanties die onlinediensten aanbieden, vereisen dat openbare instanties met inachtneming daarvan handelen. Die erkenning kan met behulp van de valideringsvoorziening plaatsvinden die thans onderdeel uitmaakt van het Ondernemersplein en die bevoegde instanties als bedoeld in de Dienstenwet faciliteert bij het valideren van elektronische handtekeningen. Die valideringvoorziening wordt waar nodig aangepast, aan de inhoud van een door de Europese Commissie op grond van de verordening vastgesteld uitvoeringsbesluit (zie verder de paragrafen 7.1 en 7.2 van deze toelichting).

De toepassing van de verordening leidt tot verwerking van persoonsgegevens. Voor wat betreft het knooppunt tot grensoverschrijdende acceptatie van elektronische identificatiemiddelen dient duidelijk te zijn wie verantwoordelijke in de zin van de Wbp is voor de verwerking van persoonsgegevens met behulp van dat knooppunt. De verantwoordelijke voor het knooppunt is de Minister van Economische Zaken. Onder zijn verantwoordelijkheid wordt het knooppunt opgezet en wordt het beheerd. De uiteindelijke positionering van dit knooppunt binnen het in ontwikkeling zijnde stelsel voor elektronische identificatie, Idensys, kan ertoe leiden dat partijen uit dit stelsel als bewerker (artikel 1, sub e, van de Wbp) van het knooppunt zullen worden aangemerkt. Het knooppunt dient in september 2018 gereed te zijn (zie verder paragrafen 8.1 en 8.2 van deze toelichting).

4. Erkenning elektronische identificatiemiddelen

4.1 Grensoverschrijdende erkenning elektronische identificatiemiddelen

De verplichting tot erkenning van elektronische identificatiemiddelen uit andere lidstaten is van toepassing op openbare instanties die toegang bieden tot onlinediensten waarvoor op grond van nationaal recht of gangbare bestuursrechtelijke praktijk elektronische identificatie met gebruikmaking van een elektronisch identificatiemiddel en authenticatie vereist is. De verplichting tot erkenning kan alleen van toepassing zijn op openbare instanties die onlinediensten aanbieden. Het begrip openbare instantie is gedefinieerd in de verordening en sluit overwegend aan bij de definitie van het begrip ‘aanbestedende dienst’ als bedoeld in de richtlijn 2014/24/EU van het Europees Parlement en de Raad van 26 februari 2014 betreffende het plaatsen van overheidsopdrachten en tot intrekking van Richtlijn 2004/18/EG (PbEU 2014, L 94). Voor de praktijk biedt het begrip aanbestedende dienst daarmee een belangrijk aanknopingspunt voor instellingen en organen om bepalen of zij een openbare instantie in de zin van de verordening zijn. Of een dienst online door een openbare instantie moet worden aangeboden en in hoeverre een elektronische identificatiemiddel daarbij vereist is, is geen onderwerp van de verordening. De verordening regelt niet de door openbare instanties geboden toegang tot elektronische dienstverlening als zodanig. Dit is een aangelegenheid van de lidstaten zelf en van eventuele andere toepasselijke Europese regelgeving. Bij online-diensten die door openbare instanties aangeboden kunnen worden, kan onder meer worden gedacht aan het online kunnen inzien van voor een burger of bedrijf bestemde (persoonlijke) informatie, het aanvragen van een vergunning, het doen van meldingen of aangiftes, het aanbrengen van wijzigingen in gegevens, de opgave van een registratie, de afwikkeling van allerlei ander opvolgend en te ontvangen retourverkeer en te verrichten handelingen. Een openbare instantie die weliswaar onlinediensten aanbiedt maar voor het gebruik waarvan geen elektronisch identificatiemiddel vereist is, hoeft geen elektronische identificatiemiddelen uit andere lidstaten te erkennen.

Niet alle elektronische identificatiemiddelen uit andere lidstaten hoeven erkend te worden. Voorwaarde voor erkenning is dat het elektronische identificatiemiddelen betreft waarvan een lidstaat het stelsel, waartoe de elektronische identificatiemiddelen behoren, heeft gemeld bij de Europese Commissie. Om grensoverschrijdend te kunnen erkennen, dienen elektronische identificatiemiddelen namelijk aan bepaalde interoperabiliteits- en veiligheidseisen te voldoen. Indien een lidstaat een stelsel niet heeft aangemeld, hoeven de openbare instanties uit een andere lidstaat de tot dat stelsel behorende elektronische identificatiemiddelen derhalve niet te erkennen.

De verplichting tot erkenning van elektronische identificatiemiddelen uit andere lidstaten, waarvan het stelsel is aangemeld bij de Commissie, is beperkt tot middelen met een vrij hoge betrouwbaarheid. De verordening onderscheidt drie betrouwbaarheidsniveaus, namelijk laag, substantieel en hoog. Deze betrouwbaarheidsniveaus zijn in een uitvoeringshandeling van de Europese Commissie nader gespecificeerd (Uitvoeringsverordening (EU) nr. 2015/1502 van de Commissie van 8 september 2015 tot vaststelling van minimale technische specificaties en procedures betreffende het betrouwbaarheidsniveau voor elektronische identificatiemiddelen overeenkomstig artikel 8, lid 3, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt (PbEU 2015, L 235)). Alleen elektronische identificatiemiddelen met een substantieel of hoog betrouwbaarheidsniveau moeten worden erkend door openbare instanties uit andere lidstaten. Daarbij geldt dat een openbare instantie nooit een elektronisch identificatiemiddel met een lager betrouwbaarheidsniveau hoeft te erkennen dan voor toegang tot de online-dienst wordt geëist.

De verplichting tot erkenning heeft tot slot betrekking op elektronische identificatiemiddelen bestemd voor natuurlijke personen, rechtspersonen of natuurlijke personen die rechtspersonen vertegenwoordigen. Rechtspersonen zijn in de zin van het Verdrag betreffende de Werking van de Europese Unie (hierna verder: VWEU) alle entiteiten die zijn opgericht naar of worden beheerst door het recht van een lidstaat, ongeacht hun rechtsvorm. Geen onderdeel van deze opsomming is de vertegenwoordiging door de ene natuurlijke persoon van een andere, zoals vertegenwoordiging in het geval van handelingsonbekwaamheid of van een onder curatele gestelde.

4.2 Uitvoeringsmaatregelen

Om grensoverschrijdend gebruik van elektronische identificatiemiddelen mogelijk te maken, is een technische voorziening nodig die berichten kan versturen over elektronische identiteiten verstrekt in Nederland en berichten kan ontvangen over elektronische identiteiten verstrekt in andere lidstaten. Deze voorziening stuurt persoonsidentificatiegegevens van burgers en bedrijven uit andere lidstaten naar Nederlandse openbare instanties die deze nodig hebben voor online dienstverlening aan deze groep. Andersom kan de voorziening persoonsidentificatiegegevens van Nederlandse burgers en bedrijven naar openbare instanties in andere lidstaten sturen, waar deze burgers en bedrijven online diensten willen afnemen, indien althans tot melding van een Nederlands stelsel bij de Europese Commissie wordt overgegaan. In voorkomend geval gaan er dan persoonsidentificatiegegevens van de Nederlandse technische voorziening naar de technische voorziening van de betreffende lidstaat. De Nederlandse technische voorziening, in feite een knooppunt, wordt aangesloten op de nationale infrastructuur elektronische identiteiten, het eID-stelsel. De technische voorziening stelt Nederlandse openbare instanties in staat om vast te stellen of het een elektronisch identificatiemiddel betreft dat is gemeld bij de Europese Commissie, over welk betrouwbaarheidsniveau dat middel beschikt en levert de authenticatie van de persoon, zodat de openbare instantie kan bepalen of toegang tot de online dienst wordt verleend. Door middel van aansluiting van het knooppunt op de bestaande Nederlandse identiteitsinfrastructuur kan het internationale berichtenverkeer via een reeds bestaande beveiligde verbinding plaatsvinden en worden onnodige inspanningen en kosten bij openbare instanties vermeden. Aangezien er wordt gewerkt met gegevens tot persoonsidentificatie is bescherming van persoonsgegevens een vereiste (zie hiervoor nader paragraaf 8 van dit deel van de toelichting). Op de verplichte erkenning door openbare instanties van elektronische identiteiten uit andere lidstaten is de Wet Naleving Europese regelgeving publieke entiteiten van toepassing. Het knooppunt dient te voldoen aan de vereisten die daaraan worden gesteld in de uitvoeringshandeling van de Europese Commissie over de interoperabiliteit van aangemelde stelsels voor elektronische identificatiemiddelen (Uitvoeringsverordening (EU) nr. 2015/1501 van de Commissie van 8 september 2015 betreffende het interoperabiliteitskader bedoeld in artikel 12, lid 8, van de Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt (PbEU 2015, L 235) (hierna verder: Uitvoeringsbesluit interoperabiliteit en knooppunt)).

4.3 De melding van een stelsel tot bewerkstelliging van erkenning

Lidstaten bepalen zelf of een stelsel, dat kan overigens ook een specifiek identificatiemiddel op een bepaald veiligheidsniveau zijn, wordt aangemeld bij de Europese Commissie. Na afronding van het notificatieproces kunnen de burgers en bedrijven hun nationale elektronische identiteit dan gebruiken voor toegang tot onlinediensten in andere lidstaten. De lidstaten moeten er zelf voor zorgen dat stelsels van elektronische identificatiemiddelen aan de bij of krachtens de verordening gestelde eisen voldoen. Een stelsel kan betrekking hebben op een elektronisch identificatiemiddel dat door of in opdracht van een lidstaat wordt uitgegeven. Een aanmelding kan ook betrekking hebben op een stelsel waarvan de daaronder vallende elektronische identificatiemiddelen onafhankelijk van de aanmeldende lidstaat worden uitgegeven, maar die door de lidstaat zijn erkend. Een stelsel kan daarmee (tevens) betrekking hebben op door de markt aangeboden elektronische identificatiemiddelen.

Bij de totstandkoming en het gebruik van een elektronisch identificatiemiddel kunnen meerdere partijen betrokken zijn met ieder een eigen verantwoordelijkheid. De partij die voor een koppeling van persoonsidentificatiegegevens aan de persoon zorg draagt, kan een andere zijn dan degene die een elektronisch identificatiemiddel uitgeeft of degene die het authenticatieproces verzorgt. De verordening bepaalt dat als tot melding bij de Europese Commissie wordt overgegaan, de lidstaat de juistheid van de persoonsidentificatiegegevens waarborgt (artikel 7d, van de verordening) en de partij die het elektronische identificatiemiddel uitgeeft verantwoordelijk is voor de koppeling tussen het middel en de identificatiegegevens van een persoon (artikel 7e, van de verordening). Daarnaast dient de aanmeldende lidstaat te voorzien in de werking en beschikbaarheid van een online authenticatievoorziening, het knooppunt, waardoor partijen die werken met elektronische identificatiemiddelen uit andere lidstaten de echtheid daarvan bevestigd kunnen krijgen op het daaraan verbonden betrouwbaarheidsniveau (artikel 7f, van de verordening). Openbare instanties moeten daarvan kosteloos

gebruik kunnen maken bij hun onlinedienstverlening aan burgers en bedrijven uit andere lidstaten. Ingeval van opzet of door nalatigheid toegebrachte schade die te wijten is aan een verzuim in de naleving van deze specifieke verplichtingen, is de lidstaat daarvoor aansprakelijk overeenkomstig de nationale regels inzake aansprakelijkheid. Voor andere in de verordening vastgestelde delen in de keten betreffende elektronische identificatiemiddelen berust aansprakelijkheid onder dezelfde voorwaarden bij de partijen die voor die delen verantwoordelijk zijn (artikel 11 van de verordening). Een lidstaat van de Europese Unie die een stelsel heeft aangemeld, dient de Europese Commissie en de andere lidstaten te informeren over veiligheidsproblemen met elektronische identiteiten van een genotificeerd stelsel. De lidstaat die het stelsel heeft aangemeld dient bij een veiligheidsinbreuk of integriteitsverlies de grensoverschrijdende authenticatie geheel of gedeeltelijk op te schorten of in te trekken (artikel 10, van de verordening). Indien de inbreuk of schending niet binnen drie maanden na deze opschorting of intrekking is verholpen, stelt de aanmeldende lidstaat de andere lidstaten en de Commissie op de hoogte van de intrekking van het stelsel voor elektronische identificatie.

4.4 Uitvoeringsmaatregelen

Burgers en bedrijven met een in Nederland uitgegeven elektronisch identificatiemiddel kunnen hiermee alleen in andere lidstaten terecht, indien het onderliggende stelsel hiervoor door Nederland is aangemeld bij de Europese Commissie. Of en wanneer Nederland een stelsel voor elektronische identificatie gaat aanmelden voor wederzijdse erkenning, is ten tijde van het opstellen van dit wetsvoorstel nog aan besluitvorming onderhevig. De besluitvorming hierin voor Nederland hangt af van nationale ontwikkelingen, in het bijzonder de totstandkoming van een stelsel voor elektronische identificatie (Idensys) waarin publieke en private aanbieders van elektronische identificatiemiddelen actief zullen zijn. Dit stelsel is thans nog in ontwikkeling. Aanmelding is voor een lidstaat facultatief en daarmee geen vereiste voor een tijdige omzetting van de verordening. De verplichting tot wederzijdse erkenning van aangemelde stelsels geldt voor alle lidstaten uiterlijk vanaf september 2018.

5. Het verlenen van vertrouwensdiensten

5.1 Het treffen van passende veiligheidsmaatregelen

Verleners van zowel niet-gekwalificeerde als gekwalificeerde vertrouwensdiensten aan het publiek verlenen diensten waarbij vertrouwen centraal staat. Gelet hierop bevat de verordening een algemeen voorschrift. Zij dienen passende technische en organisatorische maatregelen te treffen om veiligheidsrisico's van de door hen te verlenen diensten te beheersen. Het zal per vertrouwensdienst en van de beoogde betrouwbaarheid die daarmee wordt nagestreefd, afhangen op welke wijze aan deze verplichting invulling dient te worden gegeven.

5.2 Uitvoeringsmaatregelen

De verplichting voor verleners van vertrouwensdiensten passende veiligheidsmaatregelen te treffen volgt rechtstreeks uit de verordening zelf, zodat die niet in het wetsvoorstel wordt herhaald. De Europese Commissie kan door middel van uitvoeringshandelingen passende veiligheidsmaatregelen nader specificeren. Voor gekwalificeerde vertrouwensdiensten zijn de eisen in de verordening waaraan voldaan dient te zijn specifieker. Daardoor is het eenvoudiger dan voor niet-gekwalificeerde vertrouwensdiensten vast te stellen is wat passend is. Bij de invulling en uitvoering van deze norm kunnen voorts ook algemeen geaccepteerde beveiligingsstandaarden binnen de praktijk van informatiebeveiliging, zoals de Code voor Informatiebeveiliging (NEN-ISO/IEC 27002:2007 nl) van betekenis zijn. De 'richtsnoeren Beveiliging persoonsgegevens' van het College bescherming persoonsgegevens te vinden op https://cbpweb.nl/nl/richtsnoeren-beveiliging-van-persoonsgegevens-2013, gaan in op passende en organisatorische maatregelen bij de beveiliging van persoonsgegevens. Vanwege het tot dusver ontbreken van een uitvoeringshandeling hierover in de verordening zal de Minister van Economische zaken in een op artikel 4:81 van de Awb gebaseerde beleidsregel duidelijkheid verschaffen wat onder passende organisatorische en technische maatregelen voor niet-gekwalificeerde vertrouwensdiensten moet worden verstaan.

5.3 Meldplichten bij inbreuk op veiligheid of verlies van integriteit

Maatregelen die tot doel hebben de veiligheid van vertrouwensdiensten op passende wijze te waarborgen, kunnen het risico op veiligheidsinbreuken of verlies van integriteit verminderen maar niet uitsluiten. Indien zich een incident met vertrouwensdiensten voordoet, dient vertrouwen zoveel mogelijk behouden te blijven of te worden hersteld. De verordening bepaalt dat aanbieders van gekwalificeerde en niet-gekwalificeerde vertrouwensdiensten verplicht zijn een veiligheidsinbreuk of integriteitsverlies met aanzienlijke gevolgen voor de verleende vertrouwensdienst of voor de persoonsgegevens die daarmee worden beheerd binnen vierentwintig uur na ontdekking te melden bij het door een lidstaat aangewezen toezichthoudend orgaan van de lidstaat waar de verlener

gevestigd is. Waar passend dienen andere relevante organen, zoals het bevoegde nationale orgaan voor informatieveiligheid of de gegevensbeschermingsautoriteit hiervan eveneens op de hoogte te worden gesteld. Als de veiligheidsinbreuk of het integriteitsverlies waarschijnlijk negatieve gevolgen heeft voor de gebruikers, moeten deze hierover door de vertrouwensdienstverlener onmiddellijk worden geïnformeerd. Indien het algemeen belang daarmee wordt gediend, kan het toezichthoudend orgaan bepalen dat het publiek wordt of moet worden geïnformeerd over een veiligheidsinbreuk of integriteitsverlies. Doel van deze verplichtingen is het bevestigen en waar nodig herstellen van het vertrouwen van het publiek, de klanten, de markt, de overheid en de toezichthouders in de desbetreffende instelling of het desbetreffende bedrijf.

Ten algemene dient niet te snel te worden aangenomen dat een melding op grond van de verordening achterwege kan blijven. Gelet op de ernst en omvang van de gevolgen die een incident met vertrouwensdiensten kan veroorzaken, wordt aangenomen dat de verordening hierin ruim opgevat dient te worden. Dat wil zeggen dat ook sprake is van aanzienlijke gevolgen als bedoeld in de verordening indien een incident aanzienlijke gevolgen voor de verleende vertrouwensdienst kan hebben, ongeacht of het zeker is dat die zullen intreden. En in geval van gerede twijfel over de vraag hoe groot de gevolgen daadwerkelijk zouden kunnen zijn, dient eveneens tot melding te worden overgegaan. Indien daarentegen vaststaat dat een veiligheidsinbreuk of integriteitsverlies slechts beperkte impact heeft, kan een melding achterwege blijven. De verlener van vertrouwensdiensten zal in dat geval in staat zijn de inbreuk snel en adequaat te herstellen. Naarmate meer onzekerheid bestaat omtrent de aard en omvang van gevolgen van een incident voor de betrouwbaarheid of indien direct duidelijk is dat de gevolgen van een veiligheidsinbreuk of integriteitsverlies vertrouwensdiensten op grotere schaal treffen of zullen treffen, is een melding noodzakelijk.

Meldplichten zijn ook onderwerp van andere toekomstige Europese regelgeving, waaronder de meldplicht in de ontwerprichtlijn van de Europese Commissie houdende maatregelen om een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging in de Unie te waarborgen (COM (2013) 48 finaal) en in het voorstel van de Europese Commissie voor een Algemene verordening gegevensbescherming (COM (2012)11 def) ter vervanging van richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (PbEG 1995, L 281). Bij de implementatie en uitvoering van deze meldplichten zal voor zover noodzakelijk op de verhouding tot de meldplicht in de eidas-verordening worden ingegaan.

5.4 Uitvoeringsmaatregelen

De plicht tot melden van een inbreuk of integriteitsverlies is in de verordening geregeld, zodat die verplichting niet in het wetsvoorstel wordt herhaald. In het wetsvoorstel worden de in de verordening genoemde organen en autoriteit aangewezen tot wie een verplichte melding zich dient te richten. Dit zijn:
– de Minister van Economische Zaken als toezichthoudend orgaan, bedoeld in de verordening;
– de Minister van Veiligheid en Justitie (ingevolge de huidige portefeuilleverdeling de Staatssecretaris) als het nationale orgaan voor informatieveiligheid, bedoeld in de verordening;
– het College bescherming persoonsgegevens (hierna verder: Cbp) als gegevensbeschermingsautoriteit, bedoeld in de verordening.

De aanwijzing van de Minister van Economische Zaken als toezichthoudend orgaan wordt in paragraaf 7.8 toegelicht. De Minister is op grond van het wetsvoorstel bevoegd ambtenaren van Agentschap Telecom te belasten met het toezicht op het verlenen van vertrouwensdiensten. De aanwijzing van de Minister van Veiligheid en Justitie als het nationale orgaan voor informatieveiligheid volgt uit de verantwoordelijkheid van de Staatssecretaris van Veiligheid en Justitie voor het Nationaal Cyber Security Centrum (hierna verder: NCSC). De aanwijzing van het Cbp als gegevensbeschermingsautoriteit is gelegen in de verantwoordelijkheid van het Cbp voor het toezicht op de verwerking van persoonsgegevens overeenkomstig het bepaalde bij of krachtens de Wet bescherming persoonsgegevens (hierna verder: Wbp) en andere wetgeving inzake de verwerking van persoonsgegevens bepaalde (zoals art. 11.3a Tw). Met het oog daarop beschikt het Cbp over toezichthoudende en handhavende bevoegdheden (artikelen 61, 65 jo. 5:32 Awb en artikel 66 Wbp). Overigens wordt het Cbp op grond van artikel 51, vierde lid, Wbp met ingang van 1 januari 2016 in het maatschappelijk verkeer aangeduid als: Autoriteit persoonsgegevens. Ter gelegenheid van de implementatie van de Algemene verordening gegevensbescherming zal deze nieuwe aanduiding in de wetgeving worden doorgevoerd.

De meldplichten in de verordening leiden tot samenloop met andere geregelde of in voorbereiding zijnde meldplichten in nationale wet- en regelgeving. Het betreft achtereenvolgens de meldplicht uit het op de Tw gebaseerde Besluit elektronische handtekeningen aan ACM en NCSC, de in artikel 34a van de Wbp vastgelegde meldplicht aan het Cbp en de in het wetsvoorstel Wet gegevensverwerking

en meldplicht cybersecurity te regelen meldplicht aan het NCSC. Het wetsvoorstel brengt de in nationale wet- en regelgeving geregelde meldplichten in overeenstemming met de rechtstreekse werkende meldplichten op grond van de verordening. Daartoe vervallen meldplichten in wet- en regelgeving, uitsluitend voor zover die op verleners van vertrouwensdiensten van toepassing zijn.

De meldplicht in het Besluit elektronische handtekeningen heeft betrekking op aanbieders van gekwalificeerde certificaten voor elektronische handtekeningen aan het publiek. Een melding van certificatiedienstverleners dient op grond van dat besluit gericht te zijn aan ACM en aan de Staatssecretaris van Veiligheid en Justitie als verantwoordelijke voor het NCSC. Tevens zijn in dat besluit de gegevens geduid die bij een melding verstrekt dienen te worden. Deze meldplicht is na het DigiNotarincident tot stand gekomen in afwachting van de verordening. Doordat het wetsvoorstel ter uitvoering van de verordening bepaalt aan wie gemeld dient te worden en de verordening zelfstandig en met een breder toepassingsbereik bepaalt wat een meldplicht inhoudt, is het niet passend dit nog in het Besluit elektronische handtekeningen vast te leggen. Mede in het licht hiervan zal het Besluit worden heroverwogen en is het voornemen bepalingen hierover uit het Besluit te laten vervallen. Vanuit oogpunt van duidelijkheid, voorzienbaarheid en kenbaarheid kan het noodzakelijk zijn omstandigheden en criteria aan te duiden waaronder een melding vereist is. De Minister van Economische Zaken zal hierin, als verantwoordelijke voor AT, door middel van beleidsregels en/of richtsnoeren voorzien uit hoofde van het toezicht op de naleving van hoofdstuk 3 van de verordening en de Minister van Veiligheid en Justitie zo nodig voor een melding aan het NCSC.

De Wet tot wijziging van de Wbp inzake een meldplicht datalekken bevat in het nieuwe artikel 34a, eerste lid, van de Wbp, een verplichting tot melding aan het Cbp van een inbreuk op de beveiliging als bedoeld in de Wbp, die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens. Ingevolge artikel 34a, tweede lid, stelt de verantwoordelijke de betrokken personen in kennis indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer. Het Cbp zal door middel van beleidsregels de praktijk nader houvast bieden. De verordening regelt voor vertrouwensdiensten met rechtstreekse werking de meldplicht aan de nationale gegevensbeschermingsautoriteit, de mogelijkheid voor de Commissie tot duiding van daarbij over te leggen gegevens krachtens de verordening en de melding aan een betrokkene en eventueel het publiek. Dit zijn zaken die ook in de Wet tot wijziging van de Wbp inzake een meldplicht datalekken worden geregeld, zodat wordt voorgesteld de rechtstreekse werking van de verordening te respecteren en vertrouwensdiensten van het toepassingsbereik van het betreffende wetsartikel grotendeels uit te sluiten. Om zeker te stellen dat het Cbp toezicht kan houden op de naleving van de meldplichten uit de verordening, bepaalt het voorstel tot wijziging van de Tw dat het toezicht op de meldplicht ingevolge de verordening bij het Cbp wordt belegd. Dit sluit aan bij de gevolgde benadering voor het toezicht door het Cbp op de in artikel 11.3a van de Tw geregelde meldplicht betreffende persoonsgegevens voor aanbieders van openbare elektronische communicatiediensten.

Anders dan Agentschap Telecom en het Cbp is het NCSC geen toezichthouder. De activiteiten van NCSC liggen in de sfeer van het bieden van hulp en bijstand bij het waarborgen en herstellen van de beschikbaarheid en betrouwbaarheid van voor de Nederlandse samenleving vitale producten en diensten, bijvoorbeeld naar aanleiding van een vrijwillige melding. Op activiteiten van het NCSC volgend op een melding zijn bestaande wettelijke kaders van toepassing, zoals die inzake de Wbp en de Wet openbaarheid van bestuur. Naar aanleiding van de motie Hennis-Plasschaert c.s. (Kamerstukken II 2011/12, 26 643, nr. 202) is in het wetsvoorstel Wet gegevensverwerking en meldplicht cybersecurity waarin de taken van de Minister van Veiligheid en Justitie op het terrein van cybersecurity worden vastgesteld, een meldplicht geregeld voor een inbreuk op de veiligheid of een verlies van integriteit van elektronische informatiesystemen en ook het verwerken van gegevens ten behoeve van de uitvoering van die taken. In hoeverre en op welke wijze aanbieders van vertrouwensdiensten onder het toepassingsbereik van ook dat wetsvoorstel zullen vallen, is mede afhankelijk van de vraag in hoeverre deze aanbieders tevens als aanbieders van vitale diensten moeten worden aangemerkt. Hierbij is van belang dat ten tijde van de voorbereiding van het onderhavige wetsvoorstel een onderzoek loopt naar de herijking van diensten die vitaal zijn in de Nederlandse Telecomsector. De vertrouwensdiensten maken onderdeel van dit onderzoek uit. Zodra de uitkomsten van dat onderzoek bekend zijn, kan een beperkte wijziging van het wetsvoorstel nodig zijn ten behoeve van de samenloop tussen beide wetsvoorstellen.

Een verlener van vertrouwensdiensten kan op grond van de verordening verplicht zijn een incident zowel aan AT, NCSCS of ook aan het Cbp te melden. Om het risico te verkleinen dat een dienstverlener in situaties waarin snel en adequaat gehandeld dient te worden, te weinig samenhangend met meerdere van deze organen te maken krijgt bij het doen van een melding en, voor zover het AT en het Cbp betreft voor het daarop volgend toezicht, bevat het wetsvoorstel in het belang van een goede uitvoering van de verordening een samenwerkingsverplichting voor AT, NCSC en Cbp. Zij zijn verplicht een samenwerkingsprotocol af te sluiten in het belang van effectieve en efficiënte meldingen

op grond van de verordening en over het toezicht als een melding ook een inbreuk op persoonsgegevens betreft. Een dergelijk protocol kan bijvoorbeeld betrekking hebben over de wijze waarop een melding dient plaats te vinden, bijvoorbeeld via een bepaald loket. Of afspraken bevatten over het gecoördineerd organiseren van overleg met een betrokken dienstverlener naar aanleiding van een melding en het daarop volgende toezicht. Het is in het algemeen en in het bijzonder bij incidenten met urgentie van belang dat vervolg- en herstelacties niet nodeloos worden belemmerd door gebrek aan gecoördineerde afstemming tussen de aangewezen organen.

5.5 Gekwalificeerde vertrouwensdiensten en vertrouwenslijsten

Naast de algemene voorschriften die gelden voor alle verleners van vertrouwensdiensten, zijn er specifieke eisen die uitsluitend van toepassing zijn op de verleners van gekwalificeerde vertrouwensdiensten en hun diensten. Deze eisen hebben betrekking op de verlener van de vertrouwensdienst, zoals onder meer eisen betreffende personeel, procedures en betrouwbare systemen en daarnaast op de specifieke vertrouwensdienst die hij voornemens is te verlenen aan het publiek. Laatstbedoelde eisen zijn per vertrouwensdienst verschillend vastgesteld. Voor veel eisen in de verordening, waaronder ook voor gekwalificeerde vertrouwensdiensten, kan de Europese Commissie verwijzen naar private referentienormen die invulling geven aan gestelde eisen. Het voldoen aan deze normen levert het vermoeden op dat aan die eisen van de verordening is voldaan. Normen maken de algemene eisen specifiek, controleerbaar en toetsbaar. Normen worden opgesteld door internationale en Europese normalisatie organisaties zoals ISO en ETSI. Het is niet verplicht de referentienormen waarnaar wordt verwezen na te leven voor het verlenen van gekwalificeerde vertrouwensdiensten. Andere werkwijzen die een vergelijkbaar resultaat opleveren zijn ook toegestaan.

Een verlener van vertrouwensdiensten die het voornemen heeft gekwalificeerde vertrouwensdiensten aan het publiek te verlenen dient een kennisgeving van zijn voornemen te doen aan het toezichthoudend orgaan. Doordat aan gekwalificeerde vertrouwensdiensten een hoge mate van betrouwbaarheid wordt toegekend, is van belang dat deskundige externe toetsing op de in de verordening gestelde eisen plaatsvindt onverminderd de noodzaak van publiekrechtelijk toezicht. Bij de kennisgeving van het voornemen dient een conformiteitsbeoordelingsverslag van een conformiteitsbeoordelingsinstantie worden overgelegd dat op de verlener en de dienst betrekking heeft. Bij een conformiteitsbeoordelingsinstantie zijn auditors werkzaam die deskundig zijn op het terrein van vertrouwensdiensten. Een dergelijke instantie moet geaccrediteerd zijn overeenkomstig Verordening (EG) nr. 765/2008 van het Europees Parlement en de Raad van 9 juli 2008 tot vaststelling van de eisen inzake accreditatie en markttoezicht betreffende het verhandelen van producten en tot intrekking van Verordening (EEG) nr. 339/93 (PbEU 2008, L 218). Accreditatie vindt plaats aan de hand van geharmoniseerde accreditatienormen. De Europese Commissie is bevoegd vast te stellen welke van deze normen geschikt zijn voor de accreditatie van conformiteitsbeoordelingsinstanties die de hiervoor genoemde audit willen uitvoeren. Tevens kan de Europese Commissie regels vaststellen voor uitvoering van de audit en het conformiteitsbeoordelingsverslag. In Nederland vindt accreditatie plaats door de Raad voor Accreditatie.

Als naar het oordeel van het door de lidstaat aangewezen toezichthoudend orgaan voldaan is aan de eisen uit de verordening, kent die de status van gekwalificeerd toe aan de verlener en de desbetreffende vertrouwensdienst en wordt die status opgenomen in de vertrouwenslijst. Voor een uitbreiding van te verlenen gekwalificeerde vertrouwensdiensten is een nieuwe statustoekenning per dienst vereist. De vertrouwenslijst is een instrument met behulp waarvan een ieder elektronisch op afstand kan nagaan of de status van ‘gekwalificeerd’ nog geldig is. Momenteel bestaan er al vertrouwenslijsten voor de elektronische handtekening. Deze zullen worden uitgebreid met andere vertrouwensdiensten. Een gekwalificeerde dienstverlener die is opgenomen op de vertrouwenslijst, mag het vertrouwensmerk van de Europese Unie voor gekwalificeerde vertrouwensdiensten voeren. Dit keurmerk is een eenvoudige, herkenbare en duidelijke manier om in de hele Europese Unie aan te geven dat een vertrouwensdienst gekwalificeerd is. Ook na opname in de vertrouwenslijst moet de gekwalificeerde verlener en de gekwalificeerde dienst aan de eisen uit de verordening blijven voldoen.

De verlener van vertrouwensdiensten die is opgenomen in de vertrouwenslijst en daarmee gekwalificeerde certificaten mag afgeven, kan op grond van de verordening een afgegeven certificaat intrekken. Indien dit zich voordoet, registreert de verlener deze intrekking in zijn certificatendatabank en maakt hij de ingetrokken status van het certificaat tijdig, en in elk geval binnen 24 uur na ontvangst van het verzoek, bekend. De intrekking wordt onmiddellijk na de bekendmaking ervan van kracht. De verlener verstrekt aan elke vertrouwende partij informatie over de geldigheid of ingetrokken status van door hem afgegeven gekwalificeerde certificaten. Deze informatie dient op elk moment, en ook na de geldigheidsduur van het certificaat, in ieder geval per certificaat beschikbaar te zijn in een geautomatiseerde vorm die betrouwbaar, kosteloos en efficiënt is. Minder vergaand dan intrekking is tijdelijke schorsing van certificaten. De verordening bepaalt dat lidstaten regelgeving kunnen vaststellen over de tijdelijke schorsing van gekwalificeerde certificaten voor gekwalificeerde elektronische handtekeningen en gekwalificeerde elektronische zegels. In de internationale ETSI standaarden wordt de



mogelijkheid van het opschorten van certificaten – naast het intrekken – feitelijk nu al geboden, maar het ondersteunen daarvan door gekwalificeerde vertrouwensdienstverleners is optioneel. De gedachte achter het opschorten is dat iemand de status van een certificaat niet vertrouwt en de vertrouwensdienstverlener daarover inlicht. De vertrouwensdienstverlener wil deze melding verifiëren bij de certificaathouder en gedurende die tijd schort de vertrouwensdienstverlener het certificaat op. Wanneer er niets aan de hand blijkt te zijn dan wordt het certificaat weer geldig gemeld en anders definitief ingetrokken.

5.6 Uitvoeringsmaatregelen

Doordat in de verordening specifieke eisen worden gesteld aan gekwalificeerde verleners van vertrouwensdiensten en hun diensten, is het niet langer mogelijk in nationale regelgeving eisen voor te schrijven waaraan voldaan dient te worden. In het wetsvoorstel vervalt de grondslag die de Tw biedt om bij of krachtens algemene maatregel van bestuur eisen te stellen aan certificatiedienstverleners van gekwalificeerde certificaten voor het publiek en aan hun gekwalificeerde certificaten. Dit zal gevolgen hebben voor het Besluit elektronische handtekeningen. De verordening biedt nog wel ruimte voor nationale regelgeving als het gaat om de verificatie van de identiteit van degene aan wie een gekwalificeerd certificaat wordt afgegeven. De huidige Tw regelt de verificatie van de identiteit voor gekwalificeerde certificaten die op naam van natuurlijke personen worden gesteld, die bestemd zijn voor elektronische handtekeningen en waarbij identificatie in fysieke aanwezigheid plaatsvindt. Dat dient plaats te vinden aan de hand van de bij de Wet op de identificatieplicht aangewezen geldige documenten. Als gevolg van de verordening strekt verificatie zich voortaan ook uit tot andere soorten gekwalificeerde certificaten en ook tot rechtspersonen en daarnaast tot de gevallen waarin online-identificatie en -authenticatie toegestaan is. Voorgestelde wijzigingen van de Tw bepalen hoe verificatie in die gevallen dient plaats te vinden. Dit omvat ook de verificatie van zogenoemde attributen, extra specifieke gegevens die op een persoon betrekking hebben, en die van een certificaat deel kunnen uitmaken.

Te onderscheiden van in de verordening vastgestelde eisen zijn normen die deze eisen specifiek en controleerbaar maken. Voor het waarborgen van de betrouwbaarheid en de rechtszekerheid is noodzakelijk dat bij de toepasselijkheid van de verordening vanaf 1 juli 2016 in voldoende mate is voorzien in dergelijke veelal technische normen, waaraan een vermoeden van overeenstemming met de eisen kan worden ontleend. Aangezien het aanwijzen van normen geen verplichting maar een bevoegdheid van de Europese Commissie is, kan het voorkomen dat er wel normen voorhanden zijn maar dat deze niet zijn aangewezen. Gelet hierop bepaalt het wetsvoorstel dat bij of krachtens algemene maatregel van bestuur hierin kan worden voorzien, voor zover dit voor een goede uitvoering van de verordening is vereist.

Op grond van de huidige Tw kan de Minister van Economische Zaken een of meer organisaties aanwijzen die bevoegd zijn certificatiedienstverleners te toetsen op overeenstemming met eisen die bij en krachtens deze wet aan hen en hun diensten zijn gesteld, en die daartoe een bewijs van toetsing kunnen afgeven. Het betreft een ingevolge het Besluit elektronische handtekeningen geaccrediteerde organisatie. De aangewezen organisatie onderhoudt samen met andere belanghebbenden een certificatieschema dat het TTP.NL-schema wordt genoemd. Dit schema is op basis van zelfregulering tot stand gekomen. Het bewijs van toetsing van een aangewezen organisatie wordt gelet hierop ook wel de TTP-verklaring genoemd. Indien een certificatiedienstverlener over een dergelijk bewijs van toetsing van een door de Minister aangewezen organisatie beschikt, wordt daaraan het vermoeden ontleend dat aan de krachtens de Tw gestelde eisen is voldaan. In plaats daarvan kan een certificatiedienstverlener ook zelf bewijs aandragen waaruit blijkt dat aan de krachtens de wet gestelde eisen is voldaan. In de praktijk wordt van deze laatste mogelijkheid geen gebruik gemaakt.

Deze in de Tw geregelde systematiek is niet langer houdbaar onder de verordening. De verordening maakt het mogelijk dat een conformiteitsbeoordeling uitgevoerd kan worden door een geaccrediteerde conformiteitsbeoordelingsinstantie uit een andere lidstaat. Dit heeft als voordeel dat vertrouwensdienstverleners minder afhankelijk worden van de veelal schaarse nationale expertise, die soms bestaat uit één of enkele gespecialiseerde auditors die in staat zijn om een conformiteitsbeoordeling uit te voeren. Voor conformiteitbeoordelingsorganen betekent het kunnen verrichten van conformiteitsbeoordelingen van gekwalificeerde vertrouwensdienstverleners in andere lidstaten een aanzienlijke vergroting van de markt. Het door de minister kunnen aanwijzen van conformiteitbeoordelingsinstanties op basis van nationale toelatingseisen past niet binnen de gedachte van grensoverschrijdende dienstverlening van geaccrediteerde conformiteitsbeoordelingsorganen en vervalt daarom in het wetsvoorstel. Het stellen van nationale eisen aan conformiteitbeoordelingsorganen kan als belemmering voor toegang tot de Nederlandse markt worden beschouwd. De toezichthouder dient zich er bewust van te zijn dat hierdoor tussen conformiteitsbeoordelingsinstanties verschillen kunnen optreden. Daarnaast is er niet langer sprake van vrijwillige maar van verplichte inschakeling van een conformiteitsbeoordelingsinstantie door een verlener van vertrouwensdiensten

die de status gekwalificeerd wil hebben of heeft verkregen. De verordening kent bovendien aan de beschikbaarheid van een verslag of verklaring van een conformiteitsbeoordelingsinstantie geen vermoeden toe dat sprake is van overeenstemming met de in de verordening gestelde eisen. Vanuit de behoefte aan beter en meer direct toezicht op verleners van vertrouwensdiensten naar aanleiding van het incident met DigiNotar in 2011, is continuering van toekenning van een positief bewijsvermoeden aan een verslag of verklaring van de conformiteitsbeoordelingsinstantie ook niet wenselijk. In het wetsvoorstel komen de bepalingen over dit bewijsvermoeden daardoor te vervallen.

Voorgestelde wijzigingen in de Telecommunicatiewet hebben daarnaast betrekking op het opstellen en bijhouden van een nationale vertrouwenslijst door het toezichthoudend orgaan. Gekwalificeerde dienstverleners die op de vertrouwenslijst geregistreerd staan en gekwalificeerde vertrouwensdiensten aanbieden, zijn op grond van de verordening bevoegd tot intrekking van een afgegeven certificaat. Gelet op de rechtstreekse werking van de verordening is dit geen onderwerp van het wetsvoorstel. Evenmin bevat het wetsvoorstel bepalingen over het opschorten van certificaten. In Nederland wordt van de mogelijkheid tot het opschorten van certificaten geen gebruik gemaakt. Er is geen behoefte om deze lijn te wijzigen. In het (private) programma van eisen PKI-overheid is vastgelegd dat het niet toegestaan is certificaatopschorting te ondersteunen.

5.7 Toezicht en handhaving

Lidstaten zijn verplicht een toezichthoudend orgaan aan te wijzen. Een toezichthoudend orgaan moet toezien op de naleving van de eisen uit de verordening over vertrouwensdiensten, maar bijvoorbeeld ook de vertrouwenslijst opstellen en bijhouden. De verordening maakt onderscheid in toezicht op niet-gekwalificeerde en gekwalificeerde vertrouwensdiensten. Het toezicht op niet-gekwalificeerde vertrouwensdiensten is beperkt tot het toezicht op het treffen van passende en technische organisatorische maatregelen en vindt uitsluitend achteraf plaats in reactie op klachten, kennisgeving of incidenten. Aan deze vorm van beperkt toezicht liggen op Europees niveau onder meer overwegingen van uitvoerbaarheid en beperking van administratieve lasten ten grondslag.

Het toezicht op gekwalificeerde verleners van vertrouwensdiensten is zwaarder ingericht. Toezicht vindt vooraf en vervolgens structureel plaats en strekt zich uit tot de specifieke eisen. Voordat een verlener een gekwalificeerde vertrouwensdienst mag verlenen, dient hij het voornemen hiertoe kenbaar te maken aan het toezichthoudend orgaan. Daarbij moet een conformiteitsbeoordelingsverslag worden overgelegd en beoordeelt het toezichthoudend orgaan of de status gekwalificeerd kan worden toegekend. Nadat een gekwalificeerde verlener van vertrouwensdiensten en zijn diensten eenmaal die status heeft, dient de verlener op grond van de verordening verplicht ten minste eens in de 24 maanden een nieuwe conformiteitsbeoordeling laten uitvoeren door een conformiteitsbeoordelingsorgaan (artikelen 20, tweede lid, en 21, eerste lid, van de verordening). Het toezichthoudend orgaan kan daarnaast zelf ook op elk moment een audit uitvoeren of dit op kosten van de verlener van vertrouwensdiensten laten doen. Indien er door een toezichthoudend orgaan wordt vastgesteld dat de eisen uit de verordening niet worden nageleefd, kan hij herstel daarvan binnen een gestelde termijn vorderen. Indien daaraan geen gevolg wordt gegeven kan dit leiden tot intrekking van de status gekwalificeerd. Indien er sprake blijkt te zijn van een inbreuk op de bescherming van persoonsgegevens moet de nationale gegevensbeschermingsautoriteit hierover worden geïnformeerd. Een inbreuk met mogelijk grensoverschrijdende gevolgen moet aan het betreffende land en het Europees Agentschap voor Informatieveiligheid (ENISA) worden gemeld.

Toezichthoudende organen zijn onder voorwaarden verplicht op verzoek bijstand aan elkaar te verlenen, in het bijzonder door uitwisseling van informatie. Het is mogelijk dat toezichthouders uit verschillende landen samenwerken bij een inbreuk met grensoverschrijdende gevolgen door middel van de uitvoering van een gezamenlijk onderzoek.

De lidstaten zijn verplicht voorschriften vast te stellen inzake de sancties die van toepassing zijn op inbreuken op de verordening en daarmee ook ten aanzien van vertrouwensdiensten. De vastgestelde sancties moeten doeltreffend, evenredig en afschrikkend zijn.

5.8 Uitvoeringsmaatregelen

Het toezicht op gekwalificeerde certificaten voor elektronische handtekeningen wordt momenteel op grond van de Telecommunicatiewet uitgevoerd door de ACM. Zoals hiervoor is toegelicht biedt de verordening in tegenstelling tot de richtlijn geen basis meer voor vrijwillige conformiteitsbeoordeling met toekenning van een wettelijk vermoeden dat aan eisen is voldaan. Dit heeft gevolgen voor de positie van het TTP.NL-schema dat momenteel als beoordelingsschema wordt gebruikt door (geaccrediteerde) instanties. Daarbij is door het incident met DigiNotar in 2011 duidelijk geworden dat structurele aanpassingen in het toezicht gewenst en nodig zijn. De Onderzoeksraad voor Veiligheid heeft in zijn onderzoeksrapport naar aanleiding van het incident met DigiNotar de huidige toezichtcon-

structie onverantwoord genoemd. Een aanbeveling van de Onderzoeksraad voor Veiligheid aan de Minister van Economische Zaken was om de rol van de toezichthouder aan te passen zodat er meer sprake is van daadwerkelijk toezicht. Concreet krijgt de opvolging van deze aanbeveling gestalte door het loslaten van het wettelijk geregelde vermoeden van overeenstemming (artikel 18.16a Tw). Het oordeel of al dan niet aan de eisen uit de verordening wordt voldaan is aan de toezichthouder en kan niet louter op een verslag van een conformiteitsbeoordelingsinstantie worden gebaseerd. Periodieke conformiteitsbeoordeling blijft niettemin een belangrijke rol spelen bij de uitoefening van het toezicht en is daarom verplicht gesteld in de verordening. De audit dient door een conformiteitsbeoordelingsinstantie te worden verricht en binnen drie werkdagen na afronding daarvan door de gekwalificeerde verlener van vertrouwensdiensten aan het toezichthoudend orgaan te worden verstrekt. De conformiteitbeoordelingsinstantie heeft daarbij een andere rol en verantwoordelijkheid dan de toezichthouder. De conformiteitbeoordelingsinstantie is geen verlengstuk van de toezichthouder en de audit is geen vervanging van het toezicht en de eigen oordeelsvorming van de toezichthouder. Het betekent ook dat niet de conformiteitsbeoordelingsinstantie, maar de toezichthouder bestuursorgaan is dat besluiten neemt over toelating en handhaving. Als de toezichthouder zich bijvoorbeeld voor een besluit mede baseert op de inhoud van een conformiteitsbeoordelingsverslag en de vertrouwensdienstverlener de inhoud daarvan in bezwaar of beroep ter discussie stelt, dient de toezichthouder zich hierover een zelfstandig oordeel te vormen.

De mate waarin voor het toezicht betekenisvolle conformiteitsbeoordelingsverslagen worden overlegd is mede afhankelijk van de nadere uitwerking van de verplichte conformiteitsbeoordeling en de normen waarop deze is gebaseerd. Nu is nog niet duidelijk welke vorm van conformiteitsbeoordeling, certificatie of keuring, er in Europees verband gekozen zal worden. In opdracht van de Europese Commissie wordt gewerkt aan een conformiteitbeoordelingsschema voor de verordening. Het gebruik van dit schema zal niet verplicht zijn. Er is niet voor gekozen op nationaal niveau de minister de bevoegdheid te geven een door de markt aangeboden conformiteitsbeoordelingsschema aan te wijzen. Een dergelijke aanwijzing is alleen zinvol, indien daaraan enig wettelijk vermoeden van overeenstemming kan worden ontleend. Een wettelijk vermoeden betreffende het voldoen aan eisen uit de verordening of het op juiste wijze beoordelen op het voldoen aan de eisen daaruit zou echter de mogelijkheden voor het uitoefenen van daadwerkelijk toezicht door de toezichthouder belemmeren. Dat wordt niet wenselijk geacht. De beheerder van het conformiteitbeoordelingsschema en de conformiteitsbeoordelingsinstantie zijn ervoor verantwoordelijk dat het schema en het daarop gebaseerde conformiteitsbeoordelingsverslag een volledige toetsing van de eisen van de verordening inhouden. Voor de toezichthouder moet de waarde van het verslag duidelijk zijn, zodat daarmee rekening kan worden gehouden bij de uitoefening van het toezicht. Dubbele lasten door dubbele toetsing van normen moet worden voorkomen en tegelijkertijd moet het toezicht voldoende zijn om de naleving van wet- en regelgeving effectief te borgen. Daarbij heeft de toezichthouder op grond van de verordening de bevoegdheid om ten allen tijde zelf een audit uit te voeren. Wanneer de toezichthouder dit nodig acht, zal die van deze mogelijkheid gebruik maken.

Aanpassingen in de structuur hebben ook tot heroverweging van de belegging van het toezicht geleid. Het toezicht op gekwalificeerde certificaten voor de elektronische handtekening is een taak van ACM, die tamelijk los van zijn overige activiteiten op het terrein van telecommunicatie staat. Die taak is bij de implementatie van de Richtlijn elektronische handtekeningen destijds bij de Onafhankelijke Post en Telecommunicatie Autoriteit belegd waarbij een beperkte vorm van markttoezicht uitgangspunt was en waaraan in sterke mate invulling werd gegeven door de TTP-certificering. De meer centrale positie die in de verordening aan de uitoefening van toezicht op (gekwalificeerde) vertrouwensdiensten is toebedeeld, vereist een verschuiving naar meer inhoudelijk toezicht en minder accent op toezicht dat uitsluitend procesmatig of in tweede instantie is. De ervaringen met het incident DigiNotar benadrukken de noodzaak hiervan. Een meer inhoudelijke en proactieve vorm van toezicht op het gebied van vertrouwensdiensten sluit beter aan bij de bestaande kennis, expertise en andere taken van Agentschap Telecom, een dienstonderdeel van het Ministerie van Economische Zaken. De werkzaamheden van het Agentschap in het kader van toezicht zijn vaak al gericht op specifieke technische beoordelingen -en processen, certificering, middelen/apparaten. Agentschap Telecom is bereid om hierin actief en snel te investeren. In het wetsvoorstel zijn bepalingen opgenomen die de Minister van Economische Zaken aanwijzen als toezichthoudend orgaan in de zin van de verordening, waarbij voorts is bepaald dat met het toezicht worden belast de door Minister daartoe bij besluit aangewezen ambtenaren. Daarmee zijn deze aan te wijzen ambtenaren van Agentschap Telecom toezichthouder als bedoeld in artikel 5:11 van de Awb en zijn de bevoegdheden beschikbaar, die ook voor andere toezichtstaken in de Tw geregeld zijn, zoals het door de Minister opleggen van een bestuurlijke boete (artikel 15.4, van de Tw) en, indien aan de daaraan gestelde voorwaarden is voldaan, de toepassing van bestuursdwang (artikel 15.2, van de Tw). Voorts voorziet het wetsvoorstel in bepalingen betreffende bescherming van gegevens, indien in het kader van het verplicht verlenen van bijstand gegevens worden uitgewisseld met een toezichthoudend orgaan in een andere lidstaat die betrekking hebben op een verlener van vertrouwensdiensten of zijn vertrouwensdiensten. Een lidstaat kan voorts bepalen onder welke voorwaarden het eigen toezichthoudend orgaan gezamenlijk met een toezichthoudend orgaan uit een

andere lidstaat onderzoek kan doen naar bijvoorbeeld een grensoverschrijdend incident. Gelet op het belang van grensoverschrijdend toezicht op vertrouwensdiensten, is in het wetsvoorstel voorzien onder welke voorwaarden dit mogelijk is (artikel 15.3d).

Een inhoudelijker benadering van de uitoefening van toezicht door de toezichthouder laat onverlet dat de verordening de inzet van geaccrediteerde conformiteitsbeoordelingsorganen voorschrijft (artikel 20, eerste lid, van de verordening). Daarbij is van belang op welke wijze de expertise van conformiteitsbeoordelingsorganen wordt ingezet. Een goede motivering in een verslaglegging die inzicht biedt in de wijze waarop een beoordeling tot stand is gekomen, biedt meer aanknopingspunten om tot zelfstandige oordeelsvorming op basis van een verslag te komen dan een verslag waarin dit ontbreekt (zie het Onderzoeksrapport van de Raad voor de Veiligheid, het DigiNotarincident, Waarom digitale veiligheid de bestuurstafel te weinig bereikt, 2012 te vinden op: www.onderzoeksraad.nl/uploads/items-docs/1094/Rapport_Diginotar_NL_web_def_20062012.pdf). De mate waarin voor het toezicht betekenisvolle conformiteitsbeoordelingsverslagen worden overgelegd, is mede afhankelijk van de aanwijzing van referentienormen door de Europese Commissie, zowel ten aanzien van accreditatie, auditregels als verslagen. Hierbij kan een conformiteitsbeoordelingsinstantie een audit baseren op een nog te ontwikkelen Europees conformiteitsbeoordelingsschema of het TTP-certificatieschema. Indien een schema voldoet aan de door de Europese Commissie aangewezen normen biedt dat voor AT een bepaald inzicht in de kwaliteit daarvan bij de beoordeling of aan de in de verordening gestelde eisen is voldaan. Aangezien ontwikkelingen op het gebied van informatiebeveiliging snel verlopen, is het van belang dat certificatieschema’s op basis van ervaringen en inzicht in nieuwe dreigingen worden bijgehouden.

5.9 Aansprakelijkheid

Verleners van vertrouwensdiensten bieden diensten aan die het vertrouwen in het elektronisch verkeer waarborgen. Indien een verlener van vertrouwensdiensten de verplichtingen in de verordening niet of niet volledig naleeft kan dit vertrouwen in gevaar komen of aangetast worden. Het kan tot schade voor anderen leiden. De verordening bevat voorschriften over aansprakelijkheid en bewijslast van verleners van vertrouwensdiensten. Verleners van niet-gekwalificeerde verleners van vertrouwensdiensten zijn aansprakelijk voor opzettelijk of uit onachtzaamheid toegebrachte schade aan een natuurlijke persoon of rechtspersoon die is te wijten aan een verzuim de verplichtingen uit hoofde van deze verordening na te leven. De bewijslast hiervoor ligt bij de natuurlijke persoon of de rechtspersoon. Voor verleners van gekwalificeerde verleners van vertrouwensdiensten gelden andere aansprakelijkheidsregels. De opzet of nalatigheid van een gekwalificeerde verlener van vertrouwensdiensten wordt vermoed, tenzij die bewijst dat de schade zonder opzet of nalatigheid van zijn kant is ontstaan. Teneinde de beoordeling te vergemakkelijken van het financiële risico dat verleners van vertrouwensdiensten misschien moeten dragen of dat zij zouden moeten dekken met verzekeringspolissen, laat de verordening toe dat verleners van vertrouwensdiensten, onder bepaalde voorwaarden, beperkingen verbinden aan het gebruik van de door hen verleende diensten en dat zij niet aansprakelijk zijn voor schade die het gevolg is van het gebruik van diensten dat deze beperkingen te buiten gaat. De klanten moeten vooraf terdege worden geïnformeerd over de beperkingen. Deze beperkingen moeten herkenbaar zijn voor een derde partij, bijvoorbeeld doordat er informatie over de beperkingen wordt opgenomen in de voorwaarden met betrekking tot de verleende dienst, of via andere herkenbare middelen. Om uitvoering te geven aan deze beginselen, moet deze verordening overeenkomstig de nationale aansprakelijkheidsregels worden toegepast. Daarom laat deze verordening nationale regels inzake bijvoorbeeld de definitie van schade, opzet, nalatigheid, of de toepasselijke procedurele regels, onverlet.

5.10 Uitvoeringsmaatregelen

Het ter implementatie van de Richtlijn elektronische handtekeningen opgenomen artikel 6:196b BW regelt thans de aansprakelijkheid van certificatiedienstverleners die gekwalificeerde certificaten afgegeven aan het publiek. Dit artikel legt op deze dienstverleners een gekwalificeerde schuldaansprakelijkheid met omgekeerde bewijslast (Kamerstukken II 2000/01 27 743, nr. 3, blz. 18). Indien de desbetreffende certificatiedienstverlener aan kan tonen dat hij niet nalatig heeft gehandeld, is die van zijn aansprakelijkheid ontheven. Voor dienstverleners van niet-gekwalificeerde certificaten gelden thans de nationale aansprakelijkheidsregels (het algemene aansprakelijkheidsregime van Boek 6 BW). Daar de verordening de richtlijn intrekt en in artikel 13 eigen regels met dwingende en rechtstreekse werking geeft op het terrein van de aansprakelijkheid, dient artikel 6:196b BW te vervallen.

5.11 Derde landen

In derde landen gevestigde verleners van vertrouwensdiensten kunnen binnen de Europese Unie vertrouwensdiensten verlenen. De verordening bevat geen voorschriften die daar in de weg aan staan. Een vertrouwensdienst verstrekt door een aanbieder uit een derde land wordt rechtens erkend als

gelijkwaardig aan een gekwalificeerde vertrouwensdienst verstrekt door gekwalificeerde in de Europese Unie gevestigde verleners van vertrouwensdiensten, indien die vertrouwensdienst wordt erkend op grond van een overeenkomst, gesloten tussen de Europese Unie en het betrokken derde land of een internationale organisatie, overeenkomstig een daartoe in het VWEU vastgestelde procedure (artikel 14 van de verordening). Onderwerp van die overeenkomst dient in het bijzonder te zijn dat de in een derde land gevestigde verleners van vertrouwensdiensten de binnen de Europese Unie geldende voorschriften voor gekwalificeerde verleners van vertrouwensdiensten en hun gekwalificeerde vertrouwensdiensten naleven. Ook het uitgangspunt van de wederkerigheid dient onderdeel van een dergelijke overeenkomst te zijn. Anders dan onder de richtlijn voor gekwalificeerde certificaten wordt in de verordening niet materieel geregeld aan welke eisen een verlener van vertrouwensdienst uit een derde land dient te voldoen om vertrouwensdiensten als gelijkwaardig aan gekwalificeerd te mogen aanbieden binnen de Europese Unie. Onder de verordening zijn de mogelijkheden hiervoor afhankelijk van het sluiten van een overeenkomst met de Europese Unie en van de inhoud daarvan.

5.12 Uitvoeringsmaatregelen

In artikel 3:15b BW is de regeling van de Richtlijn elektronische handtekeningen over het afgeven aan het publiek van gekwalificeerde certificaten door een certificatiedienstverlener gevestigd in een derde land, geïmplementeerd. Dit artikel noemt een aantal situaties waarin erkenning van gekwalificeerde certificaten afgegeven aan het publiek door een certificatiedienstverlener gevestigd in een derde land kan plaatsvinden. Daar de verordening de richtlijn intrekt en, zoals hierboven aangegeven, in artikel 14 regelt dat erkenning plaatsvindt op grond van een overeenkomst tussen de EU en het derde land of internationale organisatie, dient artikel 15b te worden geschrapt.

5.13 Toegankelijkheid voor personen met een handicap

Waar dat technisch mogelijk en financieel haalbaar is, zullen op grond van de verordening vertrouwensdiensten en eindgebruikersproducten die worden gebruikt bij de verlening van deze diensten toegankelijk worden gemaakt voor personen met een handicap. Voor de overheid is het voldoen aan de webrichtlijnen, waarmee de toegankelijkheid, ook voor mensen met een handicap, wordt geborgd verplicht en valt dit onder het daarin geregelde pas-toe-of leg-uit regime. Voor niet-overheden geldt deze regel niet. Bedrijven zullen de kosten van het technisch toegankelijk maken van vertrouwensdiensten voor personen met een handicap afwegen tegen bedrijfseconomische belangen. Naarmate de vraag naar toegankelijkheid van vertrouwensdiensten voor personen met een handicap groter wordt, zal de economische haalbaarheid voor specifieke aanpassingen groter zijn. Bedrijven zullen met ontwikkelingen hierin rekening dienen te houden.

6. Rechtsgevolgen bij gebruik van vertrouwensdiensten

6.1 Rechtsgevolgen en bewijs

De verordening bevat voor verschillende vertrouwensdiensten voorschriften over het rechtsgevolg en het gebruik als bewijsmiddel daarvan. Uitgangspunt van die voorschriften is dat het rechtsgevolg van een vertrouwensdienst en de toelaatbaarheid ervan als bewijsmiddel in gerechtelijke procedures niet louter ontkend mag worden op grond van het feit dat die niet aan de eisen voor een gekwalificeerde vertrouwensdienst voldoen. Dit is niet anders dan onder de Richtlijn elektronische handtekeningen. Of enige vertrouwensdienst, daargelaten of die gekwalificeerd is, tot een rechtsgevolg leidt of kan leiden is afhankelijk van nationaal recht (overweging 22). Hierop is een uitzondering. Specifiek voor de gekwalificeerde elektronische handtekening bepaalt de verordening dat die hetzelfde rechtsgevolg heeft als een handgeschreven handtekening (artikel 25, tweede lid, van de verordening). Voor andere elektronische handtekeningen dient het nationaal recht te bepalen welke rechtsgevolgen daaraan verbonden zijn (overweging 49 van de verordening). De verordening heeft het naast rechtsgevolgen ook over de toelaatbaarheid van vertrouwensdiensten als bewijsmiddel in gerechtelijke procedures. Aan verschillende gekwalificeerde vertrouwensdiensten kent de verordening voor bepaalde aspecten daarvan een vermoeden van betrouwbaarheid toe. Dit vermoeden richt zich op de integriteit of juistheid van bepaalde gegevens/functies die een bepaalde vertrouwensdienst biedt. Binnen een gerechtelijke procedure is dat van invloed op de bewijspositie tussen partijen en de bewijskracht van deze gekwalificeerde vertrouwensdiensten. Een rechtens toegekend vermoeden van juistheid en integriteit kan weerlegd worden. Tegenbewijs is dus mogelijk.

6.2 Uitvoeringsmaatregelen

In het BW is een algemene regeling opgenomen over de rechtsgevolgen van elektronische handtekeningen. Het eerste lid van 3:15a BW bepaalt dat een elektronische handtekening dezelfde rechtsgevolgen heeft als een handgeschreven handtekening indien de methode die daarbij is gebruikt voor

authentificatie voldoende betrouwbaar is, gelet op het doel waarvoor de elektronische handtekeningen werden gebruikt en op alle overige omstandigheden van het geval. In het tweede lid is het vermoeden van voldoende betrouwbaarheid neergelegd ten aanzien van de gekwalificeerde elektronische handtekening.

Daar de verordening voor de gekwalificeerde handtekening in artikel 25, tweede lid, het rechtsgevolg bepaalt, wordt de huidige regeling in artikel 3:15a over de rechtsgevolgen van de elektronische handtekening beperkt tot de geavanceerde elektronische handtekening of enig andere elektronische handtekening. Voor andere vertrouwensdiensten dan de elektronische handtekening, te weten de elektronische zegels, tijdstempels en diensten voor elektronische aangetekende bezorging, geldt dat de gekwalificeerde elektronische methode daarvan het vermoeden van integriteit en juistheid oplevert. Voor deze elektronische diensten kent ons nationaal recht geen algemene regeling over rechtsgevolgen of over het vermoeden van integriteit en juistheid. Er hoeft dan ook geen aanpassing van wetgeving plaats te vinden. De verordening vereist voor deze diensten verder geen nadere uitwerking. Wel wordt artikel 2.16 van de Awb gewijzigd als gevolg van de verordening (zie hiervoor nader de toelichting bij artikel V).

7. Erkenning van vertrouwensdiensten

7.1 Erkenning van elektronische handtekeningen en zegels

Het gebruik van een door of namens een openbare instantie aangeboden onlinedienst zoals het doorlopen van een administratieve procedure kan afhankelijk zijn gesteld van ondertekening met een elektronische handtekening (natuurlijke persoon) of het aanmaken van een elektronisch zegel (rechtspersoon). De technische invulling daarvan kan verschillen, doordat in regelgeving of door een openbare instantie zelf daaraan eisen worden gesteld. Indien een openbare instantie om technische of betrouwbaarheidsredenen uitsluitend een specifieke methode accepteert, belemmert dit de grensoverschrijdende toegang tot andere lidstaten. Burgers en bedrijven uit een andere lidstaat beschikken vaak niet over precies die methode die aan alle gestelde vereisten voldoet of het is lastig en wellicht onmogelijk die te verkrijgen. De verordening bepaalt wanneer en welke methodes grensoverschrijdend erkend dienen te worden.

De verplichting tot erkenning is van toepassing op openbare instanties die onlinediensten aanbieden, en die het gebruik daarvan afhankelijk stellen van ondertekening met een geavanceerde elektronische handtekening of het aanmaken met een geavanceerde elektronisch zegel. Deze geavanceerde vertrouwensdiensten dienen aan bepaalde in de verordening gestelde eisen te voldoen. Als voor een onlinedienst een bepaalde geavanceerde elektronische handtekening of elektronisch zegel wordt geëist of voorgeschreven, dient een openbare instantie in ieder geval ook andere geavanceerde handtekeningen en zegels te erkennen die voldoen aan door de Europese Commissie hiertoe op basis van uitvoeringshandelingen vastgestelde formats en eventueel alternatieve methodes. De technische specificaties en formats van geavanceerde elektronische handtekeningen en zegels waarvoor de verplichting tot erkenning geldt, zijn vastgelegd in het Uitvoeringsbesluit (EU) 2015/1506 van de Commissie van 8 september 2015 tot vaststelling van specificaties betreffende formaten van geavanceerde elektronische handtekeningen en geavanceerde zegels die door openbare instanties moeten worden erkend overeenkomstig respectievelijk artikel 27, lid 5, en artikel 37, lid 5, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt (PbEU 2015, L 235) (hierna verder: Uitvoeringsbesluit erkenning geavanceerde vertrouwensdiensten). Indien bij een geavanceerde elektronische handtekening of geavanceerde zegel gebruik wordt gemaakt van een ander format dan die in dit uitvoeringsbesluit worden genoemd, kan de verplichting tot erkenning door openbare instanties niettemin onder omstandigheden toch van toepassing zijn. Dat is het geval indien de lidstaat waar de door de ondertekenaar, respectievelijk de aanmaker van het zegel gebruikte verlener van vertrouwensdiensten, gevestigd is, zo mogelijk een geautomatiseerde mogelijkheid biedt om de handtekening of het zegel te valideren (artikelen 2 en 4 van het Uitvoeringsbesluit). In alle gevallen strekt de erkenning zich niet uit tot geavanceerde elektronische handtekeningen en zegels met een lagere betrouwbaarheid dan het geëiste of voorgeschreven niveau, waarbij in de verordening hieraan op een specifieke wijze invulling wordt gegeven. Een lidstaat mag verder voor grensoverschrijdend verkeer van openbare instanties die onlinediensten aanbieden geen elektronische handtekening van een hoger betrouwbaarheidsniveau dan een gekwalificeerde elektronische handtekening vereisen.

Een van de eisen die aan een geavanceerde elektronische handtekening wordt gesteld heeft betrekking op de uitsluitende controle van de aanmaakgegevens door de ondertekenaar. In de richtlijn spitst deze eis zich toe op de uitsluitende controle door de ondertekenaar over een middel, zoals een smartcard of token waarin op cryptografie gebaseerde sleutels zijn opgeslagen waarmee een elektronische handtekening kan worden aangemaakt. Dit impliceert dat de controle zich ook mede op

het beheer van de drager waarin sleutelgegevens zijn opgeslagen richt. Als gevolg van de ontwikkelingen op internet, zoals cloudoplossingen hoeft de omgeving waarin sleutelgegevens worden bewaard niet altijd onder beheer van de ondertekenaar te staan. Dit kan ook een door een derde partij beheerde omgeving zijn, zoals een informatiesysteem dat elektronisch en op afstand door de ondertekenaar te benaderen is. Het beheer en de controle over de omgeving met de sleutelgegevens verschuift hiermee naar controle op afstand van sleutelgegevens die door een ander worden beheerd. De verordening biedt hiervoor ruimte, maar stelt als voorwaarde voor een geavanceerde elektronische handtekening dat de ondertekenaar de aanmaakgegevens 'met een hoog vertrouwensniveau' onder zijn uitsluitende controle kan gebruiken. In de handreiking Betrouwbaarheidsniveaus voor elektronische overheidsdiensten (versie 3) van het Forum Standaardisatie wordt op verschillende mogelijkheden nader ingegaan.

7.2 Uitvoeringsmaatregelen

In 2011 is een voorziening gerealiseerd die bevoegde instanties als bedoeld in de Dienstenwet onder meer in staat stelt elektronische handtekeningen die aan de in dat besluit gestelde standaarden voldoet te kunnen valideren. Deze validatievoorziening elektronische handtekeningen is ondergebracht bij het digitaal Ondernemersplein. Als gevolg van de verordening zullen openbare instanties in voorkomend geval tot erkenning moeten overgaan ten aanzien van verkeer dat langs andere kanalen dan via het digitaal Ondernemersplein wordt afgewikkeld en strekt erkenning zich ook uit tot elektronische zegels. De huidige voorziening zal met de verordening in overeenstemming worden gebracht, alsmede met het verder bepaalde in het Uitvoeringsbesluit erkenning geavanceerde vertrouwensdiensten. Openbare instanties die het aangaat, zullen op deze wijze worden gefaciliteerd bij het kunnen voldoen aan de verplichtingen in de verordening over erkenning van de bedoelde vertrouwensdiensten. Dit laat onverlet dat openbare instanties zelf verantwoordelijk zijn voor de naleving van de verplichtingen inzake erkenning. Afhankelijk van de wijze waarop de bestaande voorziening wordt aangepast en gepositioneerd, kan dit inhouden dat een openbare instantie met een onlinedienst waarvoor een geavanceerde elektronische handtekening of zegel is vereist van die voorziening gebruik maakt om aan de verordening te voldoen. De validatievoorziening zal in ieder geval rekening houden met de in het Uitvoeringsbesluit erkenning geavanceerde vertrouwensdiensten vastgestelde formats. Op de naleving van de verplichtingen inzake de erkenning van genoemde elektronische handtekeningen en zegels is de Wet Naleving Europese regelgeving publieke entiteiten van toepassing.

8. Gegevensbescherming

8.1 Gegevensbescherming

De verordening bevat het algemene voorschrift dat verwerking van persoonsgegevens in overeenstemming geschiedt met Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (PbEG L 281). Deze richtlijn is geïmplementeerd in de Wet bescherming persoonsgegevens. De verwerking van persoonsgegevens is bij de uitvoering van de verordening op verschillende manieren aan de orde. Verwerking vindt plaats bij het knooppunt dat grensoverschrijdende authenticatie in het onlineverkeer met openbare instanties mogelijk moet maken, bij de afgifte en gebruik van elektronische identificatiemiddelen en vertrouwensdiensten, en bij het opstellen en bijhouden van de vertrouwenslijst.

Via het knooppunt worden persoonsidentificatiegegevens vanuit andere lidstaten omgezet naar gegevens die leesbaar zijn voor in Nederland aanwezige openbare instanties en andersom. Het knooppunt is een manier om openbare instanties uit Nederland in staat te stellen aan de verplichtingen uit de verordening over erkenning van elektronische identificatiemiddelen uit andere EU-lidstaten te voldoen. De inhoud van een minimale set aan gegevens voor grensoverschrijdend gebruik van elektronische identiteiten, is door de Europese Commissie in het Uitvoeringsbesluit interoperabiliteit en knooppunt vastgelegd. De gegevens van natuurlijke personen die het knooppunt moet verwerken zijn de voor- en achternaam, geboortedatum en een uniek identificeerbaar nummer. Dit unieke nummer bestaat uit de landcode van de Lidstaat van herkomst, de landcode van de Lidstaat van bestemming, gevolgd door een aantal leesbare karakters. Dit nummer kan per transactie verschillen en is géén Europees uniek identificerend persoonsnummer. Daarnaast maakt de uitvoeringshandeling het mogelijk aanvullende gegevens van de natuurlijke persoon met de minimale dataset mee te sturen, te weten voor- en achternaam bij geboorte, geboorteplaats, huidige adres en geslacht. Voor rechtspersonen zijn de minimale gegevens de huidige wettelijke naam en een uniek identificerend nummer. Op vrijwillige basis kunnen rechtspersonen aanvullende gegevens meesturen zoals het huidige adres en het fiscaal nummer. De openbare instantie die een dienst elektronisch verleent, is gerechtigd aanvullende gegevens te vragen om te bepalen of een ingezetene binnen de Europese Unie daadwerkelijk recht heeft om de dienst af te nemen. Deze aanvullende gegevens worden alleen

verzonden na toestemming van de gebruiker. Dit laat onverlet dat, indien gegevens niet behorend tot de genoemde verplichte of aanvullende set van gegevens, het mogelijk is andersoortige gegevens buiten het knooppunt om aan de desbetreffende overheidsdienst aan te leveren. Het knooppunt dient aan de eisen te voldoen die daaraan in het door de Commissie vastgestelde Uitvoeringsbesluit interoperabiliteit en knooppunt worden gesteld. Dit uitvoeringsbesluit bepaalt dat de bescherming van de privacy en vertrouwelijkheid van de door de knooppunten van de EU-lidstaten uitgewisselde gegevens en de handhaving van de integriteit van die gegevens wordt gewaarborgd door middel van de best beschikbare technische oplossingen en beschermingsmethoden (artikel 6, eerste lid). Het knooppunt mag geen persoonsgegevens opslaan, behalve samengevat loggegevens voor het beheer van het knooppunt (artikel 6, tweede lid, juncto artikel 9). Ook dient de integriteit en authenticiteit van de gegevens verzekerd te zijn, en met oplossingen die bij grensoverschrijdend gebruik deugdelijk zijn gebleken (artikel 7). Over beheer van beveiligingsinformatie, beveiligingsnormen en het voor de communicatie te gebruiken berichtformaat bevat het uitvoeringsbesluit voorschriften (artikelen 8 tot en met 10).

Te onderscheiden van het knooppunt is de vertrouwenslijst. De gegevens die in de vertrouwenslijst worden opgenomen hebben geen betrekking op de houders van elektronische identificatiemiddelen of van certificaten voor vertrouwensdiensten, maar op de verleners van gekwalificeerde vertrouwensdiensten en hun diensten. De vertrouwenslijst is belangrijk voor openbare instanties en andere partijen die de status van een vertrouwensdienstverlener willen controleren. Het Uitvoeringsbesluit (EU) nr. 2015/1505 van de Commissie van 8 september 2015 tot vaststelling van de technische specificaties en formaten van vertrouwenslijsten overeenkomstig artikel 22, lid 5, van de Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt (PbEU 2015, L 235) (hierna verder: Uitvoeringsbesluit vertrouwenslijsten) bevat technische specificaties waaraan de vertrouwenslijst dient te voldoen.

8.2 Uitvoeringsmaatregelen

De verwerking van persoonsgegevens dient in overeenstemming met de Wet bescherming persoonsgegevens plaats te vinden. Bijzondere aandacht bij de verwerking van persoonsgegevens geldt voor het knooppunt dat grensoverschrijdend gebruik van elektronische identiteiten mogelijk maakt. Het eIDAS-knooppunt is een technische voorziening die berichten kan versturen over elektronische identiteiten verstrekt in Nederland en berichten kan ontvangen over elektronische identiteiten verstrekt in andere lidstaten. Bij de gegevensverwerking via het eIDAS-knooppunt gaat het naast de aanvaarding van buitenlandse elektronische identiteiten door Nederlandse openbare instanties om verzending van persoonsgegevens van Nederlandse burgers en bedrijven naar openbare instanties uit andere EU-lidstaten (indien althans tot melding van een Nederlands stelsel waarop de afgifte van elektronische identificatiemiddelen berust bij de Europese Commissie wordt overgegaan). Om tijdig uitvoering te kunnen geven aan de verplichtingen uit de verordening rond erkenning van elektronische identificatiemiddelen dient het knooppunt uiterlijk medio september 2018 gereed te zijn.

Het eIDAS-knooppunt routeert versleutelde berichten met persoonsidentificatiegegevens naar openbare instanties. De beheerder van het knooppunt zal de voor openbare instanties bestemde versleutelde persoonsidentificatiegegevens hierbij evenwel niet mogen decoderen of anders dan technisch kortstondig op te slaan enkel en uitsluitend met als doel die gegevens vervolgens direct door te geleiden. Het waarborgen van de integriteit van de door te geven gegevens is onderdeel van het knooppunt. Hiertoe zullen maatregelen in het kader van bescherming van persoonsgegevens en informatiebeveiliging worden getroffen. De beveiliging betreft niet enkel technische eisen, maar ook organisatorische eisen (bijvoorbeeld periodieke audits). Het waarborgen van de juistheid van de uit het buitenland ontvangen en naar het buitenland verzonden gegevens is geen onderdeel van het knooppunt. Dit vindt plaats onder verantwoordelijkheid van de desbetreffende andere EU-lidstaat die het stelsel heeft aangemeld bij de Europese Commissie waarvan de elektronische identificatiemiddelen met bijbehorende persoonsidentificatiegegevens deel van uitmaken. Evenmin maakt de authenticatie zelf deel uit van het knooppunt. De verantwoordelijkheid voor het gebruik dat openbare instanties vervolgens na ontvangst van de gegevens maken, berust bij de openbare instanties zelf. Wel is het de bedoeling dat eIDAS-knooppunt loggegevens vastlegt om incidenten te kunnen reconstrueren, overeenkomstig het daaromtrent bepaalde in het door de Commissie vastgestelde Uitvoeringsbesluit interoperabiliteit en knooppunt. Die loggegevens mogen alleen voor met de beveiliging verenigbare doeleinden worden gebruikt. De verwerking van persoonsgegevens bij het knooppunt is noodzakelijk ter uitvoering van de verplichtingen omtrent erkenning van elektronische identificatiemiddelen in de verordening. Dit dient een goede vervulling van de publieke taak door de voor de verwerking van die persoonsgegevens verantwoordelijke in de zin van de Wbp (artikel 8, sub e, van de Wbp). Voor de verwerking van persoonsgegevens die door het knooppunt plaatsvindt dient de Minister van Economische Zaken als verantwoordelijke in de zin van artikel 1 sub d de Wbp te worden aangemerkt. Indien de Minister het feitelijk beheer van het knooppunt uitbesteed aan een

derde, bijvoorbeeld een partij uit Idensys, het in ontwikkeling zijnde nationaal stelsel voor elektronische identificatie en authenticatie van burgers en bedrijven, zal een bewerkersovereenkomst worden gesloten tussen de verantwoordelijke minister en de beheerder(s). Technisch is het namelijk mogelijk om als lidstaat meerdere knooppunten bij verschillende makelaars van Idensys te implementeren.

In het kader van de ontwikkeling van het knooppunt heeft een 'Privacy Impact Assessment' plaatsgevonden. In de 'Privacy Impact Assessment' zijn aanbevelingen gedaan en is de zwaarte van risico's ten aanzien van het knooppunt geïnventariseerd, zodat maatregelen bij de ontwikkeling van het knooppunt hierop kunnen worden afgestemd. Bij het verdere verloop van het ontwikkeltraject van het knooppunt worden, overeenkomstig het advies van het College Bescherming Persoonsgegevens, aanvullende 'Privacy Impact Assessments' uitgevoerd, hetgeen in de aanbevelingen van het onderzoek ook werd verzocht. Wat betreft belangrijke risico's in de uitgevoerde 'Privacy Impact assessment' wordt gewezen op de gevolgen voor burgers en ondernemers indien integriteitsproblemen bij het knooppunt tot aantasting van de juistheid van identiteitsgegevens zouden leiden, op de gevolgen van identiteitsdiefstal bij het knooppunt en op de gevolgen van storing bij het knooppunt waardoor termijnen voor het indienen van een aanvraag niet gehaald worden. Het intreden van dit soort situaties dient zoveel mogelijk door een adequate beveiliging voorkomen te worden en als het zich voordoet is van belang dat de burger of ondernemer weet bij wie hij terecht kan voor herstel. Om voornoemde integriteitsproblemen en identiteitsdiefstal te voorkomen worden verschillende maatregelen genomen. Ten eerste zal het knooppunt adequaat beveiligd worden conform de geldende beveiligingsstandaarden, die zoveel mogelijk op Europees niveau worden afgestemd. Verder zijn de persoonsgegevens die het knooppunt doorgeleidt, versleuteld en worden deze slechts kortstondig in het knooppunt opgeslagen. Wel zullen er gegevens worden gelogd die dienen om eventuele incidenten te detecteren en reconstrueren, zoals de identificatie van het knooppunt en het bericht, alsmede datum en tijd van het bericht. Bij de verdere doorgeleiding van de buitenlandse identiteit naar het Idensysstelsel zullen eveneens gegevens worden gelogd met als doel incidenten te detecteren en reconstrueren. Indien zich toch een incident met het knooppunt voordoet, zal per geval bezien moeten worden welke maatregelen nodig zijn. Aangezien het knooppunt geen identiteitsgegevens mag opslaan (zie artikel 6, tweede lid, juncto artikel 9, derde lid, van het Uitvoeringsbesluit interoperabiliteit en knooppunt), is het onmogelijk om alle mogelijke benadeelden in de lidstaten te informeren over een incident met het Nederlandse knooppunt. Er is sprake van een getrapte werkwijze. Lidstaten zijn verplicht om de Europese Commissie en elkaar te informeren over incidenten met elektronische identiteiten. In overleg wordt vervolgens bepaald of en op welke wijze burgers en bedrijven in de lidstaten zullen worden geïnformeerd over een incident. Lidstaten nemen vervolgens zelf de beslissing over het al dan niet intrekken van elektronische identiteiten om de gevolgen van identiteitsdiefstal voor hun burgers en bedrijven te beperken. Een burger of bedrijf is doorgaans niet op de hoogte van de werking van de infrastructuur om grensoverschrijdende identificatie en authenticatie mogelijk te maken. Een burger of bedrijf dat hiermee problemen ondervindt zal zich doorgaans tot de openbare instantie of dienstverleners wenden waar het probleem zich voordoet. Deze instanties zullen zich wenden tot de verantwoordelijke voor de identiteitsinfrastructuur en het knooppunt. De Minister kan besluiten om het knooppunt tijdelijk uit de lucht te halen om de schade te beperken. Indien daardoor termijnen niet worden gehaald, mag een burger of bedrijf hiervan niet de dupe worden. In de praktijk zal een Nederlandse openbare instantie de termijn met enkele dagen verlengen zodat alsnog aan de verplichting kan worden voldaan. Dit is in beginsel beleid dat openbare instanties zelf kunnen vaststellen. In geval er problemen zijn met het Nederlandse knooppunt die leiden tot niet beschikbaarheid zal de Minister van Economische Zaken openbare instanties verzoeken om de termijn te verlengen zodat burgers en bedrijven niet de dupe worden van problemen met het knooppunt.

Net als bij elektronische identiteiten worden bij vertrouwensdiensten persoonsgegevens verwerkt. Tijdens de registratiefase legt de vertrouwensdienstverlener persoonsgegevens van de gebruiker met de uitdrukkelijke toestemming van die gebruiker vast. De vertrouwensdienstverlener is hierbij verantwoordelijke in de zin van artikel 1, sub d, van de Wbp. Het gaat hierbij om een minimale set van gegevens waaruit blijkt aan wie de vertrouwensdienst wordt verleend. Bij persoonsgebonden vertrouwensdiensten, zoals een elektronische handtekening, verstrekt de gebruiker zelf persoonsgegevens aan de ontvangende partij. Het gaat daarbij om minimale gegevens, zoals de voor- en achternaam. Daardoor weet de ontvangende partij wie de handtekening heeft gezet. Indien er aanwijzingen zijn voor een inbreuk op de bescherming van persoonsgegevens bij het verlenen van vertrouwensdiensten door een gekwalificeerde verlener van vertrouwensdiensten, brengt Agentschap Telecom het Cbp op de hoogte van de resultaten van de audits die ten aanzien van die verlener en zijn diensten zijn uitgevoerd. De bevoegdheid en verplichting hiertoe volgt uit de rechtstreekse werking van artikel 17, vierde lid, onderdeel f, van de verordening. Een vertrouwensdienstverlener moet zelf de gegevensbeschermingsautoriteit op de hoogte stellen van een veiligheidsinbreuk of integriteitsverlies met aanzienlijke gevolgen voor de persoonsgegevens die daarmee worden beheerd. En als de inbreuk of het verlies naar verwachting negatieve gevolgen zal hebben voor een natuurlijke persoon of een rechtspersoon aan wie een vertrouwensdienst is verleend, dan moet die eveneens worden geïnformeerd. Verantwoordelijke voor de vertrouwenslijst in de zin van artikel 1, sub d, van de Wbp voor

persoonsgegevens die worden verwerkt bij het registreren van aanvragen voor het verlenen van gekwalificeerde vertrouwensdiensten, is de Minister van Economische Zaken. Artikel 2.5e van het wetsvoorstel bevestigt dit. Deze verwerking van persoonsgegevens door de Minister dient ter uitvoering van de verordening en dient een goede vervulling van de publieke taak (artikel 8, sub e, van de Wbp). Ook onder de huidige Tw vindt registratie van certificatiedienstverleners plaats. De te registreren gegevens worden vastgesteld aan de hand van uitvoeringshandelingen van de Europese Commissie die op de vertrouwenslijst betrekking hebben.

9. Aanpassingen in andere wetgeving, overgangsrecht en samenloop

9.1 Aanpassingen in andere wetgeving

In een aantal bepalingen in de wetgeving wordt verwezen naar de handtekening die voldoet aan de eisen van (het eerste en) tweede lid van artikel 3:15a BW (de eisen die worden gesteld aan de gekwalificeerde handtekening) en naar artikel 3:15b BW (afgeven van gekwalificeerde certificaten door dienstverleners uit derde landen). Deze bepalingen dienen te worden aangepast. Verwezen dient te worden naar de gekwalificeerde elektronische handtekening van artikel 3, onderdeel 12, van de verordening. De verwijzing naar het in dit wetsvoorstel geschrapte artikel 15b dient te vervallen.
Het betreft aanpassingen in Boek 7 van het Burgerlijk Wetboek, het Wetboek van Burgerlijke Rechtsvordering, de Kadasterwet, de Wet handhaving consumentenbescherming en de Wet op de omzetbelasting 1968.

9.2 Overgangsrecht

De verordening bevat overgangsrechtelijke voorschriften (artikel 51 van de verordening). Indien met toepassing van de huidige Telecommunicatiewet overeenkomstig de Richtlijn elektronische handtekeningen een gekwalificeerd certificaat is aangemaakt, dan is vanaf 1 juli 2016 dat certificaat gedurende de looptijd ervan aan te merken als gekwalificeerd certificaat voor een elektronische handtekening in de zin van de verordening. Voorts is een veilig middel waarvan overeenstemming onder de richtlijn is bepaald, vanaf 1 juli 2016 als een gekwalificeerd middel in de zin van de verordening aangemerkt. Deze bestaande certificaten en middelen vervallen niet door de verordening.

Gekwalificeerde certificaten voor elektronische handtekeningen worden onder de Richtlijn elektronische handtekeningen afgegeven door certificatiedienstverleners. Voor de status van deze dienstverleners geldt op grond van de verordening vanaf 1 juli 2016 een specifiek overgangsregime. Deze bestaande certificatiedienstverleners worden gedurende tenminste een tijdelijke periode aangemerkt als gekwalificeerde verleners van vertrouwensdiensten in de zin van de verordening. Deze status geldt minimaal totdat de dienstverlener een conformiteitsbeoordelingsverslag heeft ingediend dat door het door de lidstaat aangewezen toezichthoudend orgaan is beoordeeld. Dat verslag dient zo spoedig mogelijk doch uiterlijk 1 juli 2017 te worden ingediend. Wordt een conformiteitsbeoordelingsverslag niet tijdig overgelegd, dan wordt de aanbieder op grond van de verordening vanaf 2 juli 2017 niet langer beschouwd als gekwalificeerde verlener van vertrouwensdiensten in de zin van de verordening. De verlener beschikt dan van rechtswege niet langer over de status gekwalificeerd voor hemzelf en zijn diensten en de registratie op de vertrouwenslijst van de desbetreffende verlener van vertrouwensdiensten zal dan door het toezichthoudend orgaan ongedaan worden gemaakt. Is de uitkomst van de beoordeling van een tijdig ingediend verslag positief dan wordt de status van gekwalificeerde verlener van vertrouwensdiensten voor het verlenen van gekwalificeerde certificaten voor elektronische handtekeningen aan het publiek gehandhaafd. Totdat een tijdig ingediend verslag door het toezichthoudend orgaan is beoordeeld, is niet integraal vastgesteld dat de verlener daadwerkelijk voldoet aan de eisen die de verordening stelt aan gekwalificeerde verleners van vertrouwensdiensten en aan het verlenen van gekwalificeerde certificaten voor elektronische handtekeningen. Dat neemt niet weg dat zij als gekwalificeerde verleners van vertrouwensdiensten zijn aangemerkt, zodat de verordening op hen van toepassing is vanaf 1 juli 2016. Dit betekent dat certificatiedienstverleners vanaf 1 juli 2016 aan de bij en krachtens de verordening gestelde eisen moeten voldoen, met dien verstande dat zij een overgangsperiode hebben ten aanzien van het indienen van het conformiteitsbeoordelingsverslag. Indien een gekwalificeerde verlener van vertrouwensdiensten die voorheen een certificatiedienstverlener was aan bepaalde eisen die bij of krachtens de verordening of dit wetsvoorstel niet voldoet, dan kan de toezichthouder in het kader van de handhaving van de naleving van die eisen daartegen optreden met inachtneming van hetgeen daaromtrent in de verordening en het wetsvoorstel is bepaald.

9.3 Samenloop

Dit wetsvoorstel bevat bepalingen die de samenloop in het kader van de meldplichten regelen (zie paragraaf 5.4). Daarvan te onderscheiden is de technische samenloop tussen dit wetsvoorstel en enkele andere wetsvoorstellen die de Telecommunicatiewet wijzigen. Doordat die samenloop soms

voor ieder van die andere wetsvoorstellen op hetzelfde artikel uit de Tw betrekking heeft dat in dit wetsvoorstel wordt gewijzigd, is om pragmatische redenen er voor gekozen in een latere fase van het wetsvoorstel vast te stellen in hoeverre samenloop zich met deze wetsvoorstellen en eventueel alsdan andere ingediende wetsvoorstellen (nog) aan de orde is, wat de stand van zaken daarin is en het wetsvoorstel zo nodig alsdan hierop aan te passen. Ditzelfde geldt ten aanzien van de samenloop tussen onder meer het Burgerlijk Wetboek respectievelijk de Algemene wet bestuursrecht met het wetsvoorstel tot wijziging van het Wetboek van Burgerlijke rechtsvordering en de Algemene wet bestuursrecht in verband met vereenvoudiging en digitalisering van het procesrecht (Kamerstukken I en II, 34 059).

10. Administratieve lasten en verdere effecten voor het bedrijfsleven

De bepalingen uit de verordening kunnen gevolgen hebben voor de administratieve lasten van aanbieders van vertrouwensdiensten. Voor aanbieders van niet-gekwalificeerde vertrouwensdiensten betekent de verordening een lichte stijging van de toezichtslasten. Deze lasten treden voor de niet-gekwalificeerde aanbieders alleen op wanneer er sprake is van een vertrouwensinbreuk of integriteitsverlies bij een aanbieder. Voor aanbieders van gekwalificeerde vertrouwensdiensten betekent de verordening eveneens een stijging van administratieve lasten als gevolg van de verbreding van de scope van de verordening, de vertrouwenslijst en de meldplicht.

10.1 Elektronische identiteiten

De verplichte erkenning van elektronische identiteiten uit andere lidstaten geldt alleen voor openbare instanties in de publieke sector. De private sector kan zich aansluiten maar is dat niet verplicht. Om met elektronische identiteiten van burgers en bedrijven uit andere lidstaten om te kunnen gaan, is aansluiting op knooppunt dat inkomende en uitgaande authenticatie regelt nodig. Dit knooppunt zal worden aangesloten op de Nederlandse infrastructuur van elektronische identiteiten (eID-structuur). Op deze wijze wordt voorkomen dat openbare instanties en gebruikers uit de private sector aparte aansluitingen nodig hebben voor Nederlandse elektronische identiteiten en elektronische identiteiten uit andere lidstaten. Aansluiting van de private sector op de Nederlandse eID-infrastructuur is vrijwillig en gebeurt door een contract af te sluiten met een zogeheten herkenningsmakelaar. Het gaat hier om een contract met een privaat bedrijf. Daarnaast dient een zogeheten koppelvlak te worden gerealiseerd voor technische aansluiting. Private partijen zullen waarschijnlijk in eerste instantie op het eID-stelsel aansluiten om Nederlandse burgers en bedrijven te kunnen authentiseren. Via deze aansluiting op het eID-stelsel kan ook het berichtenverkeer van elektronische identiteiten van inwoners en bedrijven uit andere lidstaten worden afgehandeld. Dit veroorzaakt geen extra administratieve lasten of nalevingskosten.

10.2 Vertrouwensdiensten

De verordening maakt grensoverschrijdend gebruik van elektronische handtekeningen, -zegels, -tijdstempels, -diensten voor elektronisch aangetekende bezorging en certificaten voor websiteauthenticatie mogelijk, maar verplicht Nederlandse burgers of bedrijven niet tot aanschaf of tot het gebruik van deze vertrouwensdiensten. De aanbieder van een elektronische dienst of proces bepaalt of hierbij gebruik moet worden gemaakt van een elektronische handtekening, -zegel, tijdstempel, dienst voor aangetekende elektronische bezorging. De verordening bepaalt alleen dat gelijkwaardige elektronische handtekeningen, -zegels, -tijdstempels, en diensten voor aangetekende elektronische bezorging uit andere lidstaten ook moeten worden geaccepteerd. Het ontvangen van een elektronische handtekening, -zegel, -tijdstempel, dienst voor aangetekende bezorging of gebruik van een certificaat voor authenticatie van websites veroorzaakt in de regel geen extra lasten of nalevingskosten. De controle van de vertrouwensdienst verloopt meestal automatisch. Indien een ontvanger dit wenst kan hij extra controles uitvoeren, bijvoorbeeld door het gebruik van valideringsdiensten. Valideringsdiensten controleren vertrouwensdiensten op een aantal extra kenmerken waardoor extra zekerheid kan worden verkregen.

10.3 Toezichtlasten

Voor verleners van niet-gekwalificeerde vertrouwensdiensten is er sprake van stijging van lasten vanuit het nieuwe Europeesrechtelijk kader, omdat deze diensten tot nu toe niet gereguleerd zijn. De toezichtlasten vanuit de verordening worden veroorzaakt door de meldplicht bij veiligheidsinbreuken en integriteitsverlies. De hoogte van deze lasten zal samenhangen met de ernst van de inbreuk en zijn moeilijk van tevoren in te schatten. Bij een lichte inbreuk is het wellicht voldoende om de toezichthouder te informeren over de corrigerende maatregelen en zijn de lasten nihil. Een ernstige inbreuk zal gepaard gaan met hogere lasten, niet alleen door intensieve betrokkenheid van de toezichthouder, maar ook over het informeren van de klanten en het publiek.

Verleners van gekwalificeerde vertrouwensdiensten krijgen eveneens te maken met stijgende toezichtlasten. Deze worden veroorzaakt doordat de verordening meer diensten reguleert dan de Richtlijn elektronische Handtekeningen en doordat de verordening nieuwe verplichtingen introduceert. De verordening bevat een aantal verplichtingen, zoals verplichte toetsing vooraf door de toezichthouder, de periodieke conformiteitbeoordeling en meldplicht bij veiligheidsinbreuken. Daarnaast kan de toezichthouder zelf een conformiteitbeoordeling uitvoeren, vragen stellen of een controle ter plaatse uitvoeren. De tijd die de aanbieder van gekwalificeerde vertrouwensdiensten kwijt is aan registratie, de periodieke conformiteitbeoordelingen, meldingen van veiligheidsinbreuken, de periodieke bedrijfsbezoeken, meldingen van veiligheidsinbreuken en periodieke bedrijfsbezoeken, telt als administratieve lasten. Echter gelet op de huidige invulling het wettelijk kader door certificering bestonden deze lasten al voor aanbieders van gekwalificeerde elektronische handtekeningen. In de praktijk is de huidige vrijwillige accreditatieregeling dusdanig ingevuld dat voor TTP-certificatie een jaarlijkse audit bij de aanbieders van gekwalificeerde elektronische handtekeningen nodig is. Deze audit moet momenteel ook al aan de toezichthouder worden verstrekt. Daarnaast geldt voor aanbieders van gekwalificeerde elektronische handtekeningen op grond van de Telecommunicatiewet nu reeds een registratieplicht. Het Besluit Elektronische handtekeningen kent bovendien een meldplicht voor veiligheidsinbreuken en integriteitsverlies bij gekwalificeerde elektronische handtekeningen. Tot slot legde de toezichthouder onder het huidige wettelijke regime ook bedrijfsbezoeken af. Gekwalificeerde elektronische zegels, -tijdstempels, diensten van aangetekende elektronische bezorging en certificaten voor de authenticatie van websites zijn tot nu toe niet gereguleerd. Doordat deze onder de verordening komen te vallen, wordt het toezichtregime van toepassing. Dit betekent voor de aanbieders van deze diensten administratieve lasten die men tot nu toe niet heeft. Deze lasten worden, net als bij de gekwalificeerde elektronische handtekening, veroorzaakt door toetsing van de toezichthouder voordat de dienst mag worden verleend, periodieke conformiteitbeoordelingen, de vertrouwenslijst en de melding van veiligheidsinbreuken. In Nederland zijn er momenteel vier private partijen die gekwalificeerde vertrouwensdiensten leveren en drie overheidsorganisaties. Op dit moment is niet bekend in hoeverre deze partijen gekwalificeerde diensten, naast de elektronische handtekening, gaan aanbieden. Daarnaast wordt het toezichtinstrumentarium voor de nieuwe vertrouwensdiensten nog ingericht. Hierdoor is een kwantitatieve onderbouwing van de stijging van de lasten nog niet mogelijk.

11. Financiële gevolgen voor medeoverheden

Gemeenten, provincies en waterschappen moeten hun technische en organisatorische processen zodanig aanpassen dat het mogelijk is dat een burger/bedrijf zich met een elektronisch identificatiemiddel uit een andere lidstaat kan authentiseren bij een onlinedienst die voor hen toegankelijk is. Zoals in paragraaf 2 is uiteengezet, regelt de verordening niet de feitelijke toegang tot onlinediensten. De kosten voor het toegankelijk maken van processen worden dan ook niet veroorzaakt door de verordening en kunnen hier niet aan worden toegerekend. Uit onderzoek (Financiële gevolgen Europese verordening elektronische identiteiten en vertrouwensdiensten voor medeoverheden, Ecorys, 2013) blijkt dat de financiële gevolgen afhangen van het implementatiescenario dat wordt gekozen. Er wordt gekozen om het berichtenverkeer, dat samenhangt met grensoverschrijdende authenticatie, af te handelen via de in ontwikkeling zijnde voorzieningen van het Nederlandse stelsel van identificatie en authenticatie van burgers en bedrijven (Idensys). Concreet betekent dit dat het knooppunt dat het grensoverschrijdend berichtenverkeer regelt, wordt aangesloten op de zogeheten herkenningsmakelaar. Aangezien gemeenten, provincies en waterschappen op Idensys zullen aansluiten om te kunnen werken met Nederlandse elektronische identiteiten, zullen de financiële gevolgen voor het kunnen authenticeren van burgers en bedrijven uit andere lidstaten gering zijn. Het onderzoek wijst uit dat het gaat om eenmalige kosten ter hoogte van ongeveer driehonderdduizend Euro en jaarlijkse kosten die minder dan honderdduizend Euro voor alle gemeenten, provincies en waterschappen bedragen. Conform de verplichtingen uit de Financiële Verhoudingswet zal het Ministerie van Economische Zaken deze kosten in 2018 via het Gemeente- en Provinciefonds compenseren. Vanaf september 2018 is erkenning van elektronische identiteiten uit andere lidstaten namelijk verplicht. De waterschappen vallen niet onder de Financiële Verhoudingswet en hebben derhalve geen recht op compensatie. De waterschappen kunnen meedoen aan een Europees proefproject waardoor de aansluiting via de zogeheten Connecting Europe Facility met Europese middelen kan worden gefinancierd.

12. Notificatiebeoordeling en toetsing College bescherming persoonsgegevens

Het wetsvoorstel strekt uitsluitend tot omzetting van de eidas-verordening. Notificatie van het wetsvoorstel op grond van de Richtlijn 2006/123/EG van het Europees Parlement en de Raad van 12 december 2006 betreffende diensten op de interne markt (PbEG 2006, L 376,) en de Richtlijn 98/34/EG en 98/48/EG betreffende een informatieprocedure op het gebied van normen en technische voorschriften regels betreffende de diensten van de informatiemaatschappij (PbEG 1998, L 204), zoals gewijzigd bij richtlijn 98/48/EG van 20 juli 1998 (PbEG 1998, L 217), is daarmee niet vereist.

Het wetsvoorstel is gelet op artikel 51, tweede lid, van de Wbp ter toetsing voorgelegd aan het College bescherming persoonsgegevens. Het Cbp heeft op 1 december 2015 advies uitgebracht. Het Cbp heeft zich bij de toetsing beperkt tot de ontwikkeling van het eIDAS-knooppunt. Het advies betreft het opslaan van persoonsgegevens, de verantwoordelijke voor de verwerking van persoonsgegevens, eenduidige beveiligingsmaatregelen op Europees niveau, een uitdrukkelijk wettelijke basis ingeval van gebruik van het Burger Service Nummer, de verantwoordelijkheidsverdeling bijvoorbeeld bij inbedding van het eIDAS-knooppunt binnen het in ontwikkeling zijnde Idensys-stelsel waarbij verschillende partijen verschillende verantwoordelijkheden hebben en er beperkt zicht is op het stelsel als geheel. De conclusie van het advies is dat de uit de verordening voortvloeiende verplichtingen, zoals de ontwikkeling van het eIDAS-knooppunt zorgvuldig moeten worden uitgewerkt. Het Cbp beveelt aan bij de ontwikkeling daarvan aanvullende Privacy Impact Assessments te laten uitvoeren en in de memorie van toelichting te motiveren waarom wel of geen gebruik wordt gemaakt van de beleidsruimte die de verordening op bepaalde aspecten biedt.

Met het Cbp wordt het belang van een zorgvuldige ontwikkeling van in het bijzonder het eIDAS-knooppunt en de plaats daarvan binnen het in ontwikkeling zijnde stelsel Idensys gedeeld. Met het oog hierop is tijdig met de voorbereidingen voor het eIDAS-knooppunt aangevangen, zodat er voldoende tijd is om in september 2018 een zorgvuldige ontwikkeling hiervan gereed te hebben. Naast de reeds uitgevoerde ‘Privacy Impact Assessment’ worden hiertoe aanvullende ‘Privacy Impact Assessments’ uitgevoerd ten behoeve van een zorgvuldige invoering van het eIDAS-knooppunt in de Nederlandse infrastructuur voor elektronische identificatie en authenticatie. Onder verantwoordelijkheid van de Minister van Economische Zaken wordt gewerkt aan toezicht op het hele stelsel voor elektronische identiteiten. Ook zal bij door de Europese Commissie georganiseerde expertmeetings worden aangedrongen op bindende beveiligingseisen op Europees niveau voor de eIDAS-knooppunten. Het Burger Service Nummer (BSN) zal bij grensoverschrijdende authenticatie alleen gebruikt worden indien hier een expliciete wettelijke grondslag voor is. Het Cbp beaamt voorts in het advies dat de memorie van toelichting voldoende duidelijkheid verschaft over wie verantwoordelijke in de zin van de Wbp is voor het eIDAS-knooppunt, namelijk de Minister van Economische Zaken. Tot slot is overeenkomstig het advies van het Cbp de memorie van toelichting op enkele aspecten verduidelijkt, zoals in de omzettingstabel.

13. Internetconsultatie

Van 8 juli tot en met 8 augustus 2015 is een conceptversie van de uitvoeringswet bij Europese verordening 910/2014 over elektronische identiteiten en vertrouwensdiensten (eIDAS) openbaar gemaakt in een internetconsultatie (www.internetconsultatie.nl/eidas). In totaal zijn er acht reacties ontvangen. Deze reacties zijn afkomstig van de Stichting ITrustfoundation, KPN, PWC, Connectis, Arthur’s Legal B.V., Rijksdienst voor het Wegverkeer, Unie van Waterschappen en een burger. De reacties van de internetconsultatie zijn gegroepeerd naar de onderstaande vier hoofdpunten:
- Samenhang met aanverwante ontwikkelingen;
- Toezicht en certificering;
- Aanvraag gekwalificeerde vertrouwensdienst;
- Kosten en compensatie.

Samenhang met aanverwante ontwikkelingen

Verschillende respondenten hebben gewezen op de samenhang van de verordening met andere onderwerpen, ontwikkelingen, stelsels en voorzieningen. PKI-overheid, Idensys, privacy, informatiebeveiliging, het CAB-forum, Internet of Things, data analytics en constant evoluerende cybersecurity technologieën, zijn genoemd. Daarbij wordt opgemerkt dat wetgeving niet altijd de meest effectieve manier is om spanningsvelden tussen security en privacy op te lossen.

Reactie

De onderwerpen van de verordening en het wetsvoorstel vertonen nauwe samenhang met PKI-overheid en Idensys, het in ontwikkeling zijnde Nederlandse stelsel van elektronische identiteiten voor burgers en bedrijven. Vaak worden de diensten op het gebied van elektronische identificatie door bedrijven aangeboden die ook vertrouwensdiensten leveren. Het is wenselijk dat normering, certificering, toezicht en financiering daarvan zoveel mogelijk hetzelfde wordt geregeld, zodat leveranciers niet voor iedere voorziening te maken hebben met net weer andere eisen, toezicht en bijbehorende financieringsstructuren. Bij de inrichting van het toezicht op Idensys en de mogelijke herinrichting van het toezicht op PKI-overheid zal zoveel mogelijk worden aangesloten op de normen en structuren die uit de verordening en deze uitvoeringswet voortvloeien. Daarbij moet worden onderkend dat verschillen tussen genoemde stelsels en voorzieningen kunnen leiden tot andere eisen en inrichting. Deelnemers zijn bijvoorbeeld op grond van een privaatrechtelijk contract verbonden aan de normen van PKI-overheid. Voor staatstoezicht op deze normen is een wettelijke basis nodig. Omdat het

wetsvoorstel minimumuitvoering van de verordening beoogt, is dit niet het juiste wetsvoorstel om regelingen te treffen voor Idensys of PKI-overheid. Voornoemde punten zijn onderdeel van het beleid of andere in voorbereiding zijnde wetgeving van de Ministeries van Economische Zaken en Binnenlandse Zaken en Koninkrijkrelaties.

De samenhang van het wetsvoorstel met privacy en informatiebeveiliging wordt onderkend. Een informatiebeveiligingsincident met een elektronische identiteit of vertrouwensdienst kan leiden tot een inbreuk op de bescherming van persoonsgegevens. De bescherming van persoonsgegevens en het toezicht is geregeld in de Wet bescherming persoonsgegevens (Wbp), die wordt vervangen door een voorstel van de Europese Commissie voor een Algemene verordening gegevensbescherming (COM (2012)11 def). De eidas-verordening en dit wetsvoorstel zijn onderdeel van een juridisch kader dat mede tot doel heeft informatiebeveiligingsincidenten en inbreuken op de bescherming van persoonsgegevens te voorkomen en, ingeval deze zich toch voordoen, te bestrijden.

Bij de totstandkoming van de eidas-verordening is de relatie met het CAB-Forum en de wereldwijde dimensie van internet en certificaten meerdere keren aan de orde geweest. De relatie is zowel de Nederlandse overheid als de Europese Commissie bekend. Het is juist dat de verordening noch dit wetsvoorstel van toepassing zijn op het CAB-Forum of Amerikaanse leveranciers van browsers. Dit is een complexe aangelegenheid die wordt veroorzaakt door de territoriale werking van wetgeving enerzijds en de mondiale eisen en technische werking van certificaten anderzijds. Middels handelsverdragen wordt geprobeerd om afspraken te maken over verplicht overleg tussen browserleveranciers, die buiten de Europese Unie zijn gevestigd, en een lidstaat die met een ernstig incident met certificaten te kampen heeft.

Op aanverwante ontwikkelingen zoals het Internet of Things en data analytics is ondermeer het voornoemde juridisch kader voor de bescherming van persoonsgegevens van toepassing. Los van de vraag of nadere regulering van deze aanverwante ontwikkelingen wenselijk is, is het wetsvoorstel niet de geëigende plaats om dit te doen.

Toezicht en certificering

Een aantal respondenten geeft aan dat verschillende toezichthouders en het NCSC een rol hebben bij het toezicht op de verordening en de melding en opvolging van incidenten. Respondenten wijzen op de risico's van uiteenlopende informatieverzoeken, onenigheid tussen toezichthouders bij normuitleg en tegengestelde eisen bij het optreden in geval van een crisis. Respondenten pleiten voor eenduidigheid in normering, informatie-inwinning en een gecoördineerd optreden van toezichthouders en NCSC bij een crisis. Een respondent stelt voor om in de uitvoeringswet te bepalen dat betrokken instanties samenwerkingsprotocollen moeten afsluiten waarin wordt aangegeven welk van de toezichthouders bij een crisis het initiatief neemt in de richting van betrokken vertrouwensdienstverlener(s) en hoe de gezamenlijke verantwoordelijkheden daarbij worden ingevuld.

Enkele respondenten vragen om verduidelijking van de rol en werkzaamheden van de toezichthouder ten opzichte van certificerende instellingen. Respondenten kunnen zich vinden in de in het wetsvoorstel beschreven wijziging van de rol van de toezichthouder, waarbij deze zelf een inhoudelijk oordeel vormt over het voldoen van de vertrouwensdienstverleners aan de eisen van de verordening. Respondenten geven aan dat de toezichthouder hiervoor voldoende middelen, inhoudelijke kennis en gezag moet hebben. Het toezicht dient meerwaarde te hebben en belangrijker dan de bevoegdheidstoedeling is de wijze van invulling van (toezichts-)taken. Daarbij is het belangrijk dat de toezichthouder het werk van de certificerende instellingen niet over gaat doen. Een respondent merkt op dat de frequentie van conformiteitsbeoordelingen in ISO-normen is voorgeschreven en vraagt wat de impact is wanneer buitenlandse vertrouwensdienstverleners op de Nederlandse markt verschijnen die een lagere frequentie hanteren dan in Nederland gebruikelijk is. De respondent pleit voor harmonisatie via de vast te stellen norm voor conformiteitsbeoordelingen (ETSI EN 319 103).

Reactie

Bij het toezicht op de verordening en het voorkomen en verhelpen van crisis zijn AT, het CBP en het NCSC betrokken. AT is primair verantwoordelijke voor het toezicht op de vertrouwensdienstverleners. Het CBP heeft een rol indien de bescherming van persoonsgegevens in het geding is, terwijl het NCSC hulp en ondersteuning biedt bij het verhelpen van cybersecurityincidenten. Dit zijn verschillende rollen die partijen op grond van verschillende wettelijke bevoegdheden uitoefenen. Samenwerking tussen de partijen en eenduidigheid bij optreden ingeval van een crisis is zowel in het belang van de vertrouwensdienstverleners als het oplossen van de crisis. Het voorstel om in het wetsvoorstel op te nemen dat er samenwerkingsprotocollen worden afgesloten tussen toezichthouders en het NCSC om die samenwerking beter te kunnen waarborgen wordt overgenomen (onderdeel M).

De rol van de toezichthouder is het toezien op de naleving van de verordening. Daarbij maakt de toezichthouder gebruik van risico- en dreigingsanalyses. Indien de verordening en het bepaalde in het wetsvoorstel niet wordt nageleefd kan de toezichthouder handhavend optreden. Het conformiteitbeoordelingsverslag van de conformiteitsbeoordelingsinstantie, dat gebaseerd wordt op ISO 17065, vormt de basis van het toezicht door Agentschap Telecom. Dit verslag biedt inzicht in het voldoen van de gekwalificeerde vertrouwensdienstverlener en de door hem gekwalificeerde vertrouwensdiensten aan de eisen van de verordening. Het verslag biedt geen rechtsvermoeden dat aan eisen uit de verordening is voldaan. De toezichthouder kan zelfstandig aanvullend onderzoek doen naar deelaspecten, specifieke eisen of thematisch controleren. Daarbij zal de toezichthouder dubbele inspanningen en lasten voor de vertrouwensdienstverleners zoveel mogelijk voorkomen. Dit punt van respondenten wordt onderschreven en zal in de praktijk vorm moeten krijgen. Om zijn rol te kunnen vervullen en toegevoegde waarde te kunnen bieden, is de opbouw van inhoudelijke deskundigheid bij de toezichthouder een vereiste. Het gaat om kennis van een zeer specialistisch onderwerp die in Nederland in beperkte mate aanwezig is. Het is wenselijk dat de toezichthouder deze kennis zelf in huis heeft en niet afhankelijk wordt van externe inhuur. De verordening bepaalt dat gekwalificeerde verleners van vertrouwensdiensten ten minste eens in de 24 maanden aan een conformiteitsbeoordeling onderworpen moeten worden. Deze eis dient te worden verdisconteerd in de auditschema's die worden gehanteerd. De toezichthouder kan daarnaast op ieder moment zelf een (aanvullende) audit doen. De verordening verplicht tot acceptatie van alle vertrouwensdiensten uit andere lidstaten. Voor gekwalificeerde vertrouwensdiensten uit andere lidstaten geldt, net als voor Nederlandse vertrouwensdiensten, dat deze tenminste eens in de 24 maanden aan een conformiteitsbeoordeling moeten worden onderworpen. Een aanbieder van gekwalificeerde vertrouwensdiensten afkomstig uit een lidstaat waar de toezichthouder een andere audittermijn hanteert dan de Nederlandse toezichthouder, kan zijn diensten zonder belemmering op de Nederlandse markt aanbieden. Bij het bepalen van de audittermijn zal de Nederlandse toezichthouder rekening houden met de termijn die toezichthouders in andere lidstaten bepalen.

Betrouwbaarheid gekwalificeerde vertrouwensdienst

Een respondent legt de vraag voor of zogeheten gekwalificeerde vertrouwensdiensten kunnen worden aangevraagd met een elektronische identiteit dat een 'substantieel' betrouwbaarheidsniveau heeft. Indien dit mogelijk is, beschouwt respondent dit als de introductie van een zwakke schakel in de keten. Respondent vraagt of de verordening het mogelijk maakt dat Nederland ervoor kiest om alleen een elektronische aanvraag met een elektronisch identificatiemiddel van betrouwbaarheidsniveau 'hoog' toe te staan. Een andere respondent vraagt of elektronische identiteiten als vertrouwensdiensten in de zin van de verordening kunnen worden aangemerkt.

Reactie

Artikel 24, eerste lid, van de verordening bepaalt dat een gekwalificeerd certificaat kan worden verkregen met een elektronische identiteit van niveau' substantieel' of 'hoog'. Het gaat hier om een recht dat is gekoppeld aan verplichte erkenning in andere lidstaten. Nederland kan er dan ook niet voor kiezen om alleen een afgifte van een gekwalificeerd certificaat met een elektronisch identificatiemiddel van niveau 'hoog' toe te staan. In artikel 24 eerste lid, onder b, is verder bepaald dat de fysieke aanwezigheid van de natuurlijke persoon of de gemachtigde afgevaardigde van de rechtspersoon wordt gewaarborgd voordat een gekwalificeerd certificaat wordt afgegeven. Deze waarborg zorgt ervoor dat de aanvraag en afgifte van een certificaat niet alleen op een elektronisch identificatiemiddel van niveau 'substantieel' of 'hoog' kan worden gebaseerd.

Hoewel elektronische identiteiten diensten zijn waaraan vertrouwen wordt ontleend, zijn het geen vertrouwensdiensten in de zin van verordening 910/2014 EC. De verordening geeft een limitatieve opsomming van wat vertrouwensdiensten zijn. Voor deze diensten geldt het regime van toezicht en wederzijdse erkenning, zoals in hoofdstuk 3 van de verordening is beschreven. Denkbaar is wel dat aan een elektronisch identificatiemiddel optioneel functionaliteit is toegevoegd, waardoor het tevens als een vertrouwensdienst moet worden aangemerkt. Bijvoorbeeld doordat het elektronisch identificatiemiddel naar keuze van gebruiker ook als elektronische handtekening gebruikt kan worden. In dat geval geldt hoofdstuk 2 van de verordening voor zover het middel als elektronisch identificatiemiddel geschikt is en is daarnaast het toezicht en wederzijdse erkenning uit hoofdstuk 3 van de verordening van toepassing, voor zover het middel tevens als een vertrouwensdienst kan worden gebruikt. Aangezien elektronische identiteiten nauw verwant zijn met vertrouwensdiensten en vaak door dezelfde partijen worden uitgegeven, is het wenselijk dat normering, certificering en toezicht en financiering daarvan zoveel mogelijk op dezelfde wijze vorm krijgt als bij de vertrouwensdiensten.

Kosten en compensatie

Twee respondenten vragen om in de memorie van toelichting in te gaan op de financiële gevolgen

van de verordening voor uitvoeringsorganisaties en de waterschappen. De memorie van toelichting gaat volgens hen nu alleen in op de gevolgen voor het bedrijfsleven en de medeoverheden, terwijl uitvoeringsorganisaties en de waterschappen ook kosten moeten maken. Een respondent geeft aan dat de code interbestuurlijke verhouden voorschrijft dat de waterschappen, net als gemeenten en provincies, gecompenseerd dienen te worden voor de financiële gevolgen van de verordening.

Reactie

In het onderzoek naar de financiële gevolgen van de verordening zijn de waterschappen meegenomen. De financiële gevolgen van de verordening zijn per waterschap of uitvoeringsorganisatie niet anders dan voor een gemeente of provincie. De code interbestuurlijke verhoudingen stelt dat het Rijk bij beleidsvoornemens die relevant zijn voor gemeenten en provincies inzicht geeft in de financiële consequenties, de bestuurlijke, praktische en informationele gevolgen en dat dit ook geldt voor de waterschappen. De memorie van toelichting is aangepast, zodat die inzicht biedt in de kosten van de verordening voor de waterschappen. De waterschappen zijn niet genoemd in artikel twee van de Financiële Verhoudingswet. De code Interbestuurlijke verhouding bevat evenmin een verplichting om de waterschappen te compenseren voor de kosten die implementatie van de verordening met zich meebrengt.

II. Artikelen

Onderdeel A, artikel 1.1, onderdeel ss

Voor de toepassing van het wetsvoorstel betreft het begrip vertrouwensdienst een belangrijk begrip. De definitie verwijst voor de omschrijving daarvan naar de eidas-verordening (artikel 3, onderdeel 16, van de verordening). In paragraaf 2.2 van het algemeen deel van de toelichting zijn kenmerken van verschillende vertrouwensdiensten nader toegelicht.

Onderdeel A, artikel 1.1, onderdeel tt

De verordening maakt onderscheid tussen gekwalificeerde en niet-gekwalificeerde vertrouwensdiensten. Voor gekwalificeerde vertrouwensdiensten gelden specifieke eisen en toezicht daarop. Voor niet-gekwalificeerde vertrouwensdiensten kan het niveau van betrouwbaarheid verschillend zijn.

Onderdeel A, artikel 1.1, onderdeel uu

De verlener van een vertrouwensdienst is in het wetsvoorstel gedefinieerd door te verwijzen naar de definitie die daarvan in de verordening wordt gegeven (artikel 3, onder 19, van de verordening). Het betreft een natuurlijke persoon of rechtspersoon die een of meer vertrouwensdiensten verleent.

Onderdeel A, artikel 1.1, onderdeel vv

Een gekwalificeerde verlener van vertrouwensdiensten als bedoeld in het wetvoorstel wordt in de verordening gedefinieerd als: een verlener van vertrouwensdiensten die één of meerdere gekwalificeerde vertrouwensdiensten verleent en van het toezichthoudende orgaan de status van gekwalificeerde heeft gekregen (artikel 3, onderdeel 20, van de eidas-verordening). Het is met andere woorden niet voldoende dat de verlener van vertrouwensdiensten feitelijk voldoet aan de gestelde eisen, maar noodzakelijk is ook dat de status gekwalificeerd door het toezichthoudend orgaan is toegekend. De eisen die in de verordening aan een gekwalificeerde verlener van vertrouwensdiensten worden gesteld, zijn gericht op het waarborgen van de betrouwbaarheid van een dergelijke verlener.

Onderdeel A, artikel 1.1, onderdelen ww

Evenals er gekwalificeerde vertrouwensdiensten zijn, zijn er ook gekwalificeerde certificaten. Het begrip gekwalificeerd certificaat wordt in de verordening als verzamelnaam gebruikt voor gekwalificeerde certificaten voor elektronische handtekeningen, voor elektronische zegels en voor websiteauthenticatie (artikel 3, onderdelen 15, 30 en 39). Een vertrouwensdienst waarvan een gekwalificeerd certificaat deel uitmaakt draagt bij aan een hogere betrouwbaarheid van die vertrouwensdienst.

Onderdeel A, artikel 1.1, onderdeel xx

In Verordening (EG) nr. 765/2008 van het Europees Parlement en de Raad van 9 juli 2008 tot vaststelling van de eisen inzake accreditatie en markttoezicht betreffende het verhandelen van producten en tot intrekking van Verordening (EEG) nr. 339/93 (PbEU 2008, L 218) (hierna verder te noemen: accreditatieverordening) is een conformiteitsbeoordelingsinstantie een instantie die conformiteitsbeoordelingsactiviteiten verricht, zoals onder meer ijken, testen, certificeren en inspecteren. In de

eidas-verordening dient een dergelijke instantie geaccrediteerd te zijn om een conformiteitsbeoordeling te verrichten van een gekwalificeerde verlener van vertrouwensdiensten en van de door hem verleende vertrouwensdiensten (artikel 3, onder 18, van de eidas-verordening). De accreditatie dient hierop betrekking te hebben. Daarvoor is nodig dat een nationale accreditatie-instantie op verzoek van een conformiteitsbeoordelingsinstantie beoordeelt of deze bekwaam is dit soort conformiteitsbeoordelingsactiviteiten uit te voeren. Wanneer zij bekwaam wordt bevonden, geeft de nationale accreditatie-instantie daartoe een accreditatiecertificaat af. In de Wet aanwijzing nationale accreditatie-instantie is voor Nederland de Raad voor Accreditatie als nationale accreditatie-instantie aangewezen.

Onderdeel A, artikel 1.1, onderdeel yy

In de verordening wordt het begrip gekwalificeerd middel voor het aanmaken van elektronische handtekeningen gedefinieerd. Ditzelfde geldt voor het begrip gekwalificeerd middel voor het aanmaken van elektronische zegels. Het dient te gaan om geconfigureerde software of hardware die wordt gebruikt om een elektronische handtekening of elektronisch zegel aan te maken, zoals een smartcard of een token (artikel 3, onder 22 en onder 31, van de verordening). Indien een dergelijk middel voldoet aan daaraan in de verordening gestelde eisen die op de betrouwbaarheid van dat middel betrekking hebben, is sprake van een gekwalificeerd middel (artikel 3, onder 23 en onder 32, van de verordening). In het wetsvoorstel worden deze begrippen telkens in samenhang gebruikt, zodat die in een gezamenlijk begrip zijn ondergebracht. Het aanbieden van gekwalificeerde middelen is alleen toegestaan door daartoe gecertificeerde aanbieders.

Onderdeel A, artikel 1.1, onderdeel lll

Ieder lidstaat van de Europese Unie dient een toezichthoudend orgaan als bedoeld in de verordening aan te wijzen voor de in de eigen lidstaat gevestigde verleners van vertrouwensdiensten. De taken van een toezichthoudend orgaan staan in de verordening opgesomd (artikel 17, van de verordening). Die taken beperken zich niet tot het terrein van toezicht op de naleving van de eisen uit de verordening. Dit omvat onder meer ook het verlenen van bijstand aan toezichthoudende organen uit andere lidstaten en het beoordelen of de status gekwalificeerd aan een verlener van vertrouwensdiensten en zijn vertrouwensdiensten kan worden toegekend. Elders in dit wetsvoorstel wordt de Minister van Economische Zaken aangewezen als toezichthoudend orgaan voor in Nederland gevestigde verleners van vertrouwensdiensten.

Onderdeel A, artikel 1.1, onderdeel mmm

Aan de hand van een vertrouwenslijst is voor het publiek zichtbaar welke gekwalificeerde verleners van vertrouwensdiensten en hun vertrouwensdiensten geregistreerd staan of geregistreerd zijn geweest. Een lidstaat dient een vertrouwenslijst op een veilige manier op te stellen, bij te houden en te publiceren (artikel 22 van de verordening). Een vertrouwenslijst wordt met behulp van een digitaal certificaat elektronisch ondertekend of verzegeld. Het begrip vertrouwenslijst is niet nieuw en is te herleiden tot beschikking nr. 2009/767/EG van de Europese Commissie van 16 oktober 2009 inzake maatregelen voor een gemakkelijker gebruik van elektronische procedures via het 'één-loket' in het kader van Richtlijn nr. 2006/123/EG van het Europees Parlement en de Raad betreffende diensten op de interne markt (PbEU 2009, L 274). De beschikking verplichtte lidstaten om een menselijk leesbare versie van hun vertrouwenslijst aan te bieden. Er bleek vervolgens onder meer behoefte te bestaan aan een machinaal verwerkbare versie van de vertrouwenslijst en een koppeling tussen vertrouwenslijsten. De Europese Commissie heeft daarop de beschikking gewijzigd (Wijziging van de beschikking één-loket middels het besluit nr. 2010/425/EU van de Europese Commissie van 28 juli 2010 tot wijziging van Beschikking 2009/767/EG wat betreft het opstellen, bijwerken en publiceren van vertrouwenslijsten van certificatiedienstverleners die onder toezicht staan of zijn geaccrediteerd in een lidstaat (PBEU 2010, L 199). De Europese Commissie heeft bij het vaststellen van de uitvoeringshandelingen op grond van de eidas-verordening ten aanzien van de vertrouwenslijsten het bepaalde in de aangehaalde beschikkingen als uitgangspunt genomen.

Onderdeel A, artikel 1.1, onderdeel nnn

De term 'eidas-verordening' is een veelvuldig in de praktijk gebruikte en aan de Engelse taal ontleende afkorting van de verordening. In het wetsvoorstel is deze aanduiding van de verordening overgenomen. Op vergelijkbare wijze heeft ook de roaming-verordening in de Telecommunicatiewet een plaats gekregen. De eidas-verordening biedt grondslag voor een groot aantal door de Europese Commissie vast te stellen gedelegeerde handelingen en uitvoeringshandelingen. Indien in het wetsvoorstel wordt verwezen naar de eidas-verordening is dit gelet op de gebruikte definitie daarvan met inbegrip van vastgestelde gedelegeerde handelingen en uitvoeringshandelingen.

Onderdeel B, opschrift paragraaf 2.1

In het wetsvoorstel wordt de verantwoordelijkheid voor de toekenning van de status gekwalificeerd voor vertrouwensdiensten en het opstellen en bijhouden van de vertrouwenslijst gelegd bij de Minister van Economische zaken. Die belast vervolgens ambtenaren van Agentschap Telecom met de uitvoering daarvan. De ACM blijft onverminderd verantwoordelijk voor de registratie en het bijhouden van een register voor het aanbieden van een openbaar elektronisch communicatienetwerk, een openbare elektronische communicatiedienst, dan wel bijbehorende faciliteiten. Door deze verdeling in verantwoordelijkheden en het verschil in voorschriften voor de te onderscheiden activiteiten, is in het wetsvoorstel hoofdstuk 2 van de Telecommunicatiewet opgedeeld in twee paragrafen. De eerste paragraaf heeft betrekking op openbare elektronische communicatienetwerken en -diensten, dan wel bijbehorende faciliteiten. Dit betreft de artikelen 2.1 tot en met 2.5. De tweede paragraaf heeft betrekking op gekwalificeerde vertrouwensdiensten. De artikelen in die paragraaf zijn in het wetsvoorstel nieuw toegevoegd.

Onderdeel C, artikel 2.1

Het huidige vijfde tot en met zevende lid hebben betrekking op diverse aspecten van de aanvraag van een certificatiedienstverlener tot registratie van het mogen aanbieden of afgeven van gekwalificeerde certificaten. Deze leden vervallen als gevolg van de herschikking in paragrafen en de rechtstreekse werking van de verordening. Voor zover dit voor de uitvoering van de verordening noodzakelijk is, zijn voorschriften over de toekenning van de status gekwalificeerd en de vertrouwenslijst onderdeel van de voorgestelde paragraaf over vertrouwensdiensten.

Onderdeel D, artikel 2.2

Het huidige tweede tot en met vijfde lid gaan over het weigeren, beëindigen of wijzigen van een registratie betreffende certificatiedienstverleners en gekwalificeerde certificaten. Doordat artikel 2.2 onderdeel is van paragraaf 2.1 van het wetsvoorstel en die paragraaf niet langer ook op deze doelgroep betrekking heeft, vervallen in het wetsvoorstel het derde tot en met het vijfde lid. Verder komt het tweede lid anders te luiden. In het tweede lid komt te staan wat nu is bepaald in artikel 2.2, vierde lid, onderdeel a. Daarin staat dat de ACM de registratie eindigt of wijzigt, indien de grond tot registratie is vervallen. Dit voorschrift is ook van betekenis voor aanbieders van openbare elektronische communicatienetwerken en -diensten, of bijbehorende faciliteiten. Te denken valt aan de situatie waarin een aanbieder zijn activiteiten waarop de registratie betrekking heeft uit eigener beweging beëindigt. Voor zover dit voor de uitvoering van de verordening noodzakelijk is, zijn voorschriften in verband met weigering, beëindiging of wijziging van de status gekwalificeerd bij vertrouwensdiensten onderdeel van de nieuwe in te voegen paragraaf over gekwalificeerde vertrouwensdiensten.

Onderdeel E, artikel 2.3

In de hier voorgestelde wijziging worden eerdere wijzigingen van de Telecommunicatiewet tot implementatie van het besluit van de Europese Commissie ter uitvoering van de dienstenrichtlijn over vertrouwenslijsten (zie hiervoor de toelichting bij onderdeel A, onder mmm) ongedaan gemaakt. In plaats daarvan worden de vertrouwenslijsten rechtstreeks werkend door de eidas-verordening geregeld. Noodzakelijke voorschriften ten aanzien van de vertrouwenslijst en de verantwoordelijkheid daarvoor zijn, zijn in het wetsvoorstel onderdeel van de nieuwe paragraaf over het verlenen van gekwalificeerde vertrouwensdiensten.

Onderdeel F, Artikel 2.5a

De verordening bepaalt dat die zich niet uitstrekt tot vertrouwensdiensten die uitsluitend in systemen die gesloten zijn als gevolg van nationaal recht of overeenkomsten tussen een welbepaalde groep deelnemers worden verleend (artikel 2, tweede lid, van de verordening). Gelet hierop bepaalt het voorgestelde artikel dat de Tw niet van toepassing is op de verlening van vertrouwensdiensten of op het voornemen tot verlening daarvan die van het toepassingsbereik van de eidas-verordening zijn uitgesloten. De verordening mag met name niet voorzien in de verlening van diensten die uitsluitend binnen gesloten systemen gebruikt worden tussen een welbepaalde groep deelnemers, en die geen gevolgen hebben voor derden. Systemen die zijn opgezet bij bedrijven of overheden voor het beheer van interne procedures waarbij gebruik wordt gemaakt van vertrouwensdiensten, behoren bijvoorbeeld niet onder deze verordening te vallen. Alleen vertrouwensdiensten die aan het publiek verleend worden en gevolgen hebben voor derden moeten voldoen aan de vereisten van deze verordening (overweging 21 van de verordening). Ook onder de richtlijn elektronische handtekeningen werd het toepassingsbereik ervan beperkt, waardoor systemen die berusten op vrijwillige privaatrechtelijke overeenkomsten tussen een vastgesteld aantal deelnemers zijn uitgesloten (overweging 16 van de richtlijn). In de nadere memorie van antwoord bij de Wet elektronische handtekeningen is vervolgens

aan de hand van verschillende concrete voorbeelden toegelicht hoe deze uitzondering opgevat dient te worden (Kamerstukken I 2002/03, 27 743, nr. 35b, blz. 8 tot en met 10; zie voorts ook voor gekwalificeerde certificaten en het vermelden van het toepassingsbereik daarvan in het certificaat: Kamerstukken II 2000/01, 27 743, nr. 3, blz. 19). Daarbij is tevens aangegeven dat het uiteindelijk ook het Europese Hof van Justitie is om te oordelen of sprake is van certificaten aan het publiek of niet. De desbetreffende voorbeelden en het daarbij gemaakte voorbehoud zullen naar wordt aangenomen ook onder de verordening nog steeds van betekenis zijn, met dien verstande dat die niet enkel voor gekwalificeerde certificaten voor elektronische handtekeningen relevant zijn maar voor alle vertrouwensdiensten.

Onderdeel F, Artikel 2.5b

Dit artikel betreft een nadere uitwerking van de in de eidas-verordening beschreven procedure om als gekwalificeerde verlener van vertrouwensdiensten gekwalificeerde vertrouwensdiensten te mogen aanbieden die onder het toepassingsbereik van de verordening vallen (artikel 21, van de eidas-verordening). Ter uitvoering van artikel 21 van de verordening zijn in het voorgestelde artikel voorschriften opgenomen over de kwalificatie, inhoud en behandeling van een kennisgeving van een voornemen de status gekwalificeerd te verkrijgen. De verkrijging van de status gekwalificeerd als verlener van vertrouwensdiensten geldt uitsluitend voor gekwalificeerde vertrouwensdiensten die als zodanig op de vertrouwenslijst geregistreerd staan. De status geldt niet voor niet-gekwalificeerde vertrouwensdiensten van dezelfde verlener. Indien een reeds gekwalificeerde verlener van vertrouwensdiensten meer gekwalificeerde vertrouwensdiensten wil aanbieden, dan zal de in de verordening beschreven procedure hiervoor doorlopen dienen te worden.

Uit het eerste lid volgt dat een mededeling aan de Minister van Economische Zaken van het voornemen om de status gekwalificeerd te krijgen als een aanvraag wordt aangemerkt. Het voornemen is dat de Minister ambtenaren van Agentschap Telecom met de ontvangst en behandeling van deze aanvragen zal belasten. Er wordt niet over kennisgeving maar over mededeling gesproken. Hiermee wordt hetzelfde bedoeld. Voor mededeling is gekozen vanuit oogpunt van eenheid in terminologie in hoofdstuk 2 van de Telecommunicatiewet. De kwalificatie van een mededeling als aanvraag is noodzakelijk doordat dit de basis is voor een daarop volgende inhoudelijke beoordeling door de Minister die uitmondt in een op rechtsgevolg gerichte beschikking: de toekenning respectievelijk de weigering van de status gekwalificeerd.

Het voorgestelde tweede lid vloeit voort uit het vereiste in de verordening dat de taken van het toezichthoudend orgaan, inclusief de toekenning van de status gekwalificeerd, uitsluitend betrekking hebben op de verleners van vertrouwensdiensten die gevestigd zijn in de lidstaat waarvoor het toezichthoudend orgaan is aangewezen (artikel 17, derde lid, van de verordening). De verordening licht niet toe wat onder het begrip vestiging dient te worden verstaan. De Handelsregisterwet definieert een vestiging als een gebouw of complex van gebouwen waar duurzame uitoefening van de activiteiten van een onderneming of rechtspersoon plaatsvindt (artikel 1, onderdeel j, van de Handelsregisterwet). Ook een onderneming die is opgericht naar het recht van een andere staat, maar feitelijk een hoofd- of nevenvestiging in Nederland heeft van waaruit vertrouwensdiensten worden verleend, zal in deze zin voor de toepassing van de verordening als in Nederland gevestigd te moeten worden aangemerkt. Vestiging kan aldus bijvoorbeeld geschieden door het oprichten van een dochteronderneming, het inrichten van een filiaal of het inrichten van een duurzame infrastructuur vanuit welk een economische activiteit in een lidstaat wordt ontplooid. Het tweede lid laat de toepasselijkheid van artikel 4:5, eerste lid, Awb onverlet. Indien bij een ingediende aanvraag de overlegging van een conformiteitsverslag ontbreekt, zal de Minister van Economische Zaken die aanvraag zonder dat verslag niet in behandeling nemen. De verordening stelt immers als vereiste dat een dergelijk verslag wordt overgelegd bij de kennisgeving van het voornemen. Dit verslag kan ook in een vreemde taal zijn opgesteld. In dat geval kan het voor de beoordeling van de aanvraag noodzakelijk zijn dat het desbetreffende verslag is vertaald en aan de kwaliteit van die vertaling eisen worden gesteld. Artikel 4:5, tweede lid, van de Awb, is hierop van toepassing.

Uit het derde lid volgt onder meer dat bij ministeriële regeling ook de overlegging van andere gegevens bij een aanvraag vastgesteld kunnen worden. Hierbij kan bijvoorbeeld worden gedacht aan gegevens ten aanzien van de gevolgde auditregels bij het opstellen van een verslag. Hierover kan de Europese Commissie referentienormen vaststellen (artikel 20, vierde lid, van de verordening). De aanvraag wordt door het toezichthoudend orgaan, voor Nederland is dat de Minister, beoordeeld op overeenstemming met de eisen, bedoeld in de verordening. Deze verplichting volgt rechtstreeks uit de verordening, zodat dit niet in het wetsvoorstel is overgenomen. Uit de verordening volgt voorts dat als aan die eisen naar het oordeel van het toezichthoudend orgaan is voldaan, de status van gekwalificeerd wordt verleend. Hieruit kan worden afgeleid dat als aan die eisen niet is voldaan, de toekenning van de status wordt geweigerd. De bevoegdheid tot weigering voor de Minister valt daarmee binnen de rechtstreekse werking van de verordening, zodat dit niet separaat in het wetsvoorstel is vastgelegd. Het betreft een weigeringsbesluit waartegen bezwaar en beroep kan worden ingesteld.

Het vierde lid maakt met het oog op artikel 4:13, eerste lid, van de Awb, duidelijk dat voor de beschikking op aanvraag bij wettelijk voorschrift een termijn is vastgesteld, die in de verordening is vastgesteld op drie maanden na de kennisgeving.

Onderdeel F, Artikel 2.5c

In het eerste lid wordt de Minister van Economische Zaken aangewezen als verantwoordelijke voor het opstellen, bijhouden en openbaar elektronisch toegankelijk maken van de vertrouwenslijst voor Nederland. In de huidige Tw berust die verantwoordelijkheid bij ACM. Doordat de Minister in het wetsvoorstel voor de vertrouwenslijst verantwoordelijk wordt, is de verwachting dat de toegankelijkheid van deze lijst via de website van Agentschap Telecom wordt gerealiseerd. De vertrouwenslijst dient te voldoen aan het door de Europese Commissie vastgestelde Uitvoeringsbesluit vertrouwenslijsten. Binnen het huidig wettelijk kader zijn de technische specificaties van de vertrouwenslijst en daarin op te nemen informatie geregeld in de Regeling vertrouwenslijst. De Regeling vertrouwenslijst zal als gevolg van de rechtstreekse werking van de eidas-verordening en het Uitvoeringsbesluit vertrouwenslijsten worden heroverwogen.

De Minister kan uitsluitend gegevens in de vertrouwenslijst opnemen en bijhouden, indien de gekwalificeerde verleners van vertrouwensdiensten de daarvoor benodigde juiste en volledige gegevens hebben verstrekt. Dit betreft bijvoorbeeld gegevens over de dienstverlener zelf en over de vertrouwensdiensten die zij verlenen. De verordening bepaalt niet uitdrukkelijk dat de dienstverleners die gegevens moeten verstrekken aan het voor de vertrouwenslijst verantwoordelijk orgaan. Het tweede tot en met vijfde lid voorzien in informatieverplichtingen, waardoor de Minister in staat is een vertrouwenslijst op te stellen, bij te houden en te publiceren zoals de verordening in artikel 20, tweede lid, voorschrijft. Het opstellen en bijhouden van de vertrouwenslijst en de verplichte verstrekking van gegevens zijn feitelijke handelingen en verplichtingen die niet tot een besluit leiden. Bij feitelijke onjuistheden van eenvoudige aard als bedoeld in het zesde lid, kan bijvoorbeeld worden gedacht aan kennelijke verschrijvingen of onjuistheden die geen gevolgen hebben voor de betrouwbaarheid van de lijst. Het zevende lid dient als vangnet voor het geval mocht blijken dat de uitvoeringshandelingen van de Europese Commissie over de vertrouwenslijst en de daarop te vermelden gegevens niet uitputtend zijn en tot aanzienlijke onduidelijkheid leiden.

Onderdeel F, Artikel 2.5d

De eidas-verordening bevat voorschriften over het intrekken van de status gekwalificeerd door het toezichthoudend orgaan uit hoofde van het niet naleven van de eisen uit hoofde van de verordening en over het daarvan in kennis stellen van de gekwalificeerde verlener van vertrouwensdiensten (artikel 20, derde lid, van de verordening). In het voorgestelde eerste lid wordt geregeld dat het Agentschap onverminderd hetgeen over intrekking in de verordening is bepaald over niet-naleving daarvan, de status gekwalificeerd ook om de in dat lid genoemde gevallen kan beëindigen. In onderdeel a betreft dit het handelen in strijd met het bij of krachtens de wet bepaalde ten aanzien van het verlenen van vertrouwensdiensten. Daarvan kan bijvoorbeeld sprake zijn indien niet aan de eisen is voldaan die in dit wetsvoorstel aan de vaststelling van de identiteit bij de uitgifte van een gekwalificeerd certificaat worden gesteld. Die eisen mogen ingevolge de verordening met inachtneming van het daaromtrent bepaalde overeenkomstig het nationale recht worden bepaald en zijn daarmee niet in de verordening zelf vastgesteld. Ook ingeval van strijd met die nationaal vastgestelde eisen dient beëindiging van de status gekwalificeerd tot de mogelijkheden te behoren. Het tweede lid stelt dit buiten twijfel voor de in dit wetsvoorstel opgenomen eisen. Op grond van onderdeel b kan het Agentschap tot beëindiging overgaan indien na een daartoe gestelde termijn de gegevens waarnaar in dat onderdeel wordt verwezen niet alsnog zijn verstrekt. Het betreft gegevens die op grond van het wetsvoorstel door de gekwalificeerde verleners van vertrouwensdiensten verstrekt dienen te worden aan het Agentschap, zodat die aan zijn verplichtingen ten aanzien van het opstellen en bijhouden van de vertrouwenslijst kan voldoen. Ook hiervoor geldt dat buiten iedere twijfel wordt gesteld dat bij niet-naleving van deze verplichting, na een daartoe gestelde termijn, tot beëindiging van de status gekwalificeerd moet kunnen leiden. Anders kan het vertrouwen van het publiek in de vertrouwenslijst of in relatie tot de betrokken verlener geschaad worden.

Onderdeel F, Artikel 2.5e en onderdeel G, artikel 11.5b

De in het kader van een aanvraag ontvangen gegevens kunnen persoonsgegevens bevatten. Voor zover dat het geval is en die gegevens onderdeel worden van een gegevensverzameling, is op grond van het voorgestelde onderdeel F de Minister daarvoor verantwoordelijke in de zin van de Wet bescherming persoonsgegevens. Dit geldt ook met betrekking tot de persoonsgegevens die in de vertrouwenslijst voorkomen. Op grond van de verordening is opname van informatie over de gekwalificeerde verleners van vertrouwensdiensten in de vertrouwenslijst en openbaarmaking van die lijst verplicht (artikel 22, eerste lid, van de verordening), zodat de hiervoor benodigde gegevens niet

afgeschermd mogen worden. Het betreft in voorkomend geval een zeer beperkte set gegevens, betreffende vooral naam, woonplaats en adres. Het voornemen is dat Agentschap Telecom met de hiervoor benodigde gegevensverwerkingen zal worden belast. De in onderdeel G voorgestelde wijzigingen hebben betrekking op het verbreden van de werkingssfeer van artikel 11.5b tot verleners van vertrouwensdiensten. Naast de toepasselijkheid van de Wet bescherming persoonsgegevens, wordt met de voorgestelde onderdelen tevens nadere invulling gegeven aan artikel 5 van de eidas-verordening.

Onderdeel H, artikel 11.5c

De verordening bevat een rechtstreeks werkende meldplicht voor verleners van vertrouwensdiensten ingeval van incidenten met vertrouwensdiensten die zich ook uitstrekt tot het doen van een melding aan de nationale gegevensbeschermingsautoriteit. Die meldplicht is aan de orde bij een inbreuk op de veiligheid of verlies van integriteit met aanzienlijke gevolgen voor de persoonsgegevens die met een vertrouwensdienst worden beheerd (zie artikel 19, tweede lid, van de eidas-verordening). Ook de melding aan een natuurlijke persoon of rechtspersoon die naar verwachting negatieve gevolgen zal hebben van een inbreuk of integriteitsverlies is rechtstreeks werkend in de verordening vastgesteld. Over de bij een melding te overleggen gegevens kan de Europese Commissie uitvoeringshandelingen vaststellen. In dit onderdeel wordt het Cbp als nationale gegevensbeschermingsautoriteit aangewezen. Voor de bij een melding te overleggen gegevens, indien de Europese Commissie geen uitvoeringshandelingen hierover vaststelt, wordt verwezen naar de toelichting bij onderdeel P.

Onderdeel I, artikel 15.1

Dit onderdeel maakt het mogelijk ambtenaren van Agentschap Telecom te belasten met het toezicht op hoofdstuk III van de verordening. Het huidige artikel 15.1 bepaalt wie met het toezicht op de naleving van het bij of krachtens de Telecommunicatiewet bepaalde belast is. Voor de in het eerste lid opgesomde activiteiten en onderwerpen worden met het toezicht op de naleving van de daarop betrekking hebbende voorschriften belast de bij besluit van Onze Minister aangewezen ambtenaren (voor zover het althans bevoegdheden van de Minister aangaat). De daarvoor aangewezen ambtenaren maken deel uit van het dienstonderdeel Agentschap Telecom. De voorgestelde wijzigingen hebben tot gevolg dat de opsomming aan activiteiten en onderwerpen in het eerste lid wordt verruimd tot het toezicht op de naleving van de bepalingen in het deel van de eidas-verordening dat over vertrouwensdiensten gaat en tot enkele bepalingen in het wetsvoorstel over vertrouwensdiensten. Dit toezicht beperkt zich tot in Nederland gevestigde verleners van vertrouwensdiensten en hun vertrouwensdiensten aan het publiek. Bij de uitoefening van het toezicht zal Agentschap Telecom onderscheid dienen te maken tussen verleners van gekwalificeerde respectievelijk niet-gekwalificeerde vertrouwensdiensten. Ten aanzien van niet-gekwalificeerde verleners van vertrouwensdiensten is Agentschap Telecom op grond van de verordening uitsluitend bevoegd achteraf te handhaven op basis van een signaal dat een niet-gekwalificeerde verlener van vertrouwensdiensten of de door hem verleende vertrouwensdienst niet zou voldoen aan de vereisten van de verordening (artikel 17, derde lid, onderdeel b, van de verordening).

Het huidige artikel 15, derde lid, van de Telecommunicatiewet, is vastgesteld bij Wet van 4 juni 2015 tot wijziging van de Wet bescherming persoonsgegevens en enige andere wetten in verband met de invoering van een meldplicht bij de doorbreking van maatregelen voor de beveiliging van persoonsgegevens alsmede uitbreiding van de bevoegdheid van het College bescherming persoonsgegevens om bij overtreding van het bepaalde bij of krachtens de Wet bescherming persoonsgegevens een bestuurlijke boete op te leggen (Stb. 2015, 230). Het artikellid bepaalt dat het Cbp toezicht houdt op de naleving van artikel 11.3a, waardoor dit toezicht ziet op voorschriften die betrekking hebben op een inbreuk op de beveiliging die nadelige gevolgen heeft voor de bescherming van persoonsgegevens die zijn verwerkt in verband met de levering van openbare elektronische communicatiediensten. Het hier voorgestelde artikel 15.1, derde lid, breidt het toezicht van het Cbp uit tot artikel 11.5b dat betrekking heeft op de verwerking van persoonsgegevens door verleners van vertrouwensdiensten en tot de meldplicht als geregeld in artikel 19, tweede lid, verordening voor een inbreuk op de veiligheid of het verlies van integriteit van persoonsgegevens waarbij vertrouwensdiensten betrokken zijn (zie hiervoor nader paragraaf 5.4, van het algemeen deel). Het Cbp is daarmee geen toezichthoudend orgaan als bedoeld in artikel 17, eerste lid, van de verordening. Hiervan te onderscheiden is het toezicht op de naleving van het samenstel aan voorschriften uit de verordening waarvoor een lidstaat een toezichthoudend orgaan als bedoeld in artikel 17, eerste lid, van de verordening dient aan te wijzen (zie hiervoor de toelichting op onderdeel L) en waarvan het voornemen is dat de Minister van Economische Zaken het Agentschap Telecom daarmee zal belasten.

Onderdeel J, artikel 15.3b

Aan het verlenen van vertrouwensdiensten zijn vaak grensoverschrijdende aspecten verbonden. Een

verlener van vertrouwensdiensten kan bijvoorbeeld in de ene lidstaat van de Europese Unie gevestigd zijn en in een andere lidstaat zijn diensten aanbieden. Of de servers waarvan gebruikt wordt gemaakt, bijvoorbeeld voor het aanmaken van certificaten, staat niet in de lidstaat van vestiging van de verlener van vertrouwensdiensten maar in een andere lidstaat (zie overweging 42 van de verordening). De eidas-verordening bepaalt dat toezichthoudende organen verplicht zijn samen te werken voor het uitwisselen van goede praktijken met betrekking tot vertrouwensdiensten (artikel 18 van de verordening). Een verzoek tot bijstand dient gemotiveerd zijn. Wederzijdse bijstand kan in het bijzonder betrekking hebben op informatieverzoeken en toezichthoudende maatregelen, zoals verzoeken om inspecties uit te voeren in verband met de conformiteitsbeoordelingsverslagen. Een toezichthoudend orgaan mag een verzoek om bijstand weigeren vanwege een limitatief aantal in de verordening opgesomde redenen.

Uit het eerste lid volgt dat de ambtenaren die belast zijn met het toezicht op de in Nederland gevestigde verleners van vertrouwensdiensten ook belast zijn met het verlenen van bijstand. Het verlenen van bijstand zal zich in het bijzonder concentreren op het verschaffen van informatie en gegevens die voor een toezichthoudend orgaan uit een andere lidstaat behulpzaam zijn bij de uitoefening van het toezicht door dat orgaan op de in die andere lidstaat gevestigde verleners van vertrouwensdiensten. Om deze bijstand te kunnen te verlenen in overeenstemming met de verordening, dienen de aangewezen ambtenaren van Agentschap Telecom over de daarvoor benodigde bevoegdheden te beschikken ten aanzien van verleners van vertrouwensdiensten die in Nederland actief zijn, maar hier niet gevestigd zijn en waarop het verzoek tot bijstand betrekking heeft. Het betreft bevoegdheden zoals het vorderen van inlichtingen, het inzien of kopiëren van gegevens en bescheiden, onderzoek van apparatuur en voorzieningen, en zo nodig door inspectie ter plaatse. Deze bevoegdheden en de voorwaarden waaronder die gebruikt mogen worden zijn in titel 5.2 van de Awb geregeld voor toezichthouders als bedoeld in artikel 5:11 van die wet. De ambtenaren belast met het verlenen van bijstand, treden evenwel strikt genomen niet op als toezichthouder voor in andere lidstaten gevestigde verleners van vertrouwensdiensten waarop een verzoek tot bijstand betrekking heeft. Op grond van het voorgestelde tweede lid kunnen de aangewezen ambtenaren die belast zijn met het verlenen van bijstand hun toezichtsbevoegdheden ook voor bijstand gebruiken. Hiervan is uitgezonderd artikel 5:19 van de Awb dat betrekking heeft op het onderzoeken van vervoermiddelen. Het is niet aannemelijk dat het gebruik van deze bevoegdheid noodzakelijk is. Het voorgestelde derde lid heeft betrekking op de toepassing van de bestuurlijke boete bij overtreding van artikel 5:20, van de Awb. Daarin is bepaald dat een ieder verplicht aan een toezichthouder binnen de door hem gestelde redelijke termijn alle medewerking dient te verlenen die deze redelijkerwijs kan vorderen bij de uitoefening van zijn bevoegdheden.

Onderdeel J, artikel 15.3c

Bij een verzoek tot het verlenen van bijstand stelt de Minister van Economische Zaken vast of een weigeringsgrond in de verordening van toepassing is. Een verzoek wordt niet opgevolgd, indien de Minister niet bevoegd is om de gevraagde bijstand te leveren, de gevraagde bijstand niet in verhouding staat tot de toezichthoudende activiteiten van de door de Minister daarmee belaste ambtenaren van Agentschap Telecom, of het aanbieden van de gevraagde bijstand onverenigbaar is met de verordening (artikel 18, tweede lid, van de verordening). De Minister heeft op grond van het het voorgestelde eerste lid in ieder geval niet de bevoegdheid de gevraagde bijstand te verlenen, indien de geheimhouding van mogelijke bedrijfsvertrouwelijke gegevens en inlichtingen na verstrekking daarvan naar zijn oordeel onvoldoende gewaarborgd is. Dit laat onverlet dat een verzoek ook op een van de andere in de verordening genoemde gronden kan worden afgewezen. Het aanbieden van de gevraagde bijstand kan bijvoorbeeld als onverenigbaar met de verordening worden beschouwd (artikel 18, tweede lid, onderdeel c, van de verordening), indien niet voldoende is gewaarborgd dat gegevens of inlichtingen uitsluitend worden gebruikt door het toezichthoudende orgaan van wie het verzoek tot bijstand afkomstig is ten behoeve van een juiste naleving van de eidas-verordening.

Onderdeel J, artikel 15.3d

Indien van toepassing kunnen lidstaten hun toezichthoudende organen toestaan gezamenlijke onderzoeken uit te voeren waarbij personeelsleden van toezichthoudende organen van andere lidstaten betrokken zijn. De regelingen en procedures voor dergelijke gezamenlijke acties worden door de betrokken lidstaten overeenkomstig hun wetgeving overeengekomen en vastgelegd (artikel 18, derde lid, van de verordening). Lidstaten dienen op grond van de verordening in voorkomend geval de mogelijkheid tot het doen van gezamenlijk onderzoek te kunnen toestaan. Gelet op het grensoverschrijdend karakter van het verlenen van vertrouwensdiensten, is het van belang dat deelname door ambtenaren van Agentschap Telecom aan een gezamenlijk onderzoek openstaat. Het voorgestelde artikel bepaalt wanneer dat kan en wat daarbij geldt.

Voorwaarde voor een gezamenlijk onderzoek is dat tussen het toezichthoudend orgaan in de andere

lidstaat en de Minister van Economische Zaken hierover overeenstemming is bereikt. Hierop hebben het eerste en tweede lid betrekking. Het kan gaan om situaties waarin een incident heeft plaatsgevonden bij een verlener van vertrouwensdiensten die grensoverschrijdend actief is. Onder omstandigheden kan het dan zinvol zijn dat ambtenaren van Agentschap Telecom in nauw en direct overleg met collega's van een toezichthoudend orgaan uit een andere lidstaat treden over de aanpak van een onderzoek, de uitvoering daarvan en het uitwisselen van informatie die tijdens en na een onderzoek wordt verkregen. Bij ernstige incidenten waarbij behoefte is aan snelle en hoogwaardige kennisuitwisseling, kan er bovendien behoefte aan bestaan dat een ter zake deskundige persoon werkzaam bij een ander toezichthoudend orgaan op locatie informatie kan inzien, beoordelen en vervolgvragen kan voorleggen aan Agentschap Telecom en omgekeerd ook zelf nieuwe informatie kan delen met het Agentschap. Gelet hierop beschikken de ambtenaren van Agentschap Telecom die aan een gezamenlijk onderzoek deelnemen op grond van het derde lid over dezelfde bevoegdheden als bij het verlenen van bijstand. Ook kan een ambtenaar van Agentschap Telecom met een beroep op artikel 5:15, derde lid, van de Awb, zijn bevoegdheden uitoefenen in aanwezigheid van een persoon die werkzaam is bij een toezichthoudend orgaan uit een andere lidstaat. Een persoon die voor een toezichthoudend orgaan uit een andere lidstaat aan een gezamenlijk onderzoek deelneemt mag vervolgens van gegevens en inlichtingen kennis nemen onder de voorwaarden die daaraan zijn verbonden. De bevoegdheid tot het vorderen van gegevens en inlichtingen en de verantwoordelijkheid voor inspectie ter plaatse blijft uitsluitend berusten bij de betrokken ambtenaren van Agentschap Telecom.

Onderdeel K, artikel 16.1

De Minister van Economische Zaken dient werkzaamheden of diensten te verrichten ter uitvoering van het bepaalde in de eidas-verordening. De Minister wordt in het wetsvoorstel aangewezen als toezichthoudend orgaan en is daarmee verantwoordelijk voor het vervullen van in de verordening aan dat orgaan toegekende taken. De inhoud van die taken zijn echter niet bij of krachtens dit wetsvoorstel bepaald, maar in de eidas-verordening zelf. Daardoor kan onduidelijkheid bestaan of de werkzaamheden of diensten die de Minister ter uitvoering van de eidas-verordening verricht eveneens onder het toepassingsbereik van de algemene vergoedingsregeling kunnen vallen. De voorgestelde wijzigingen in dit artikel geven hierover uitdrukkelijk uitsluitsel. Ten aanzien van niet-gekwalificeerde vertrouwensdiensten vindt geen registratie plaats van de verleners van die diensten en zijn de verdere werkzaamheden van een andere omvang en orde dan in verband met gekwalificeerde vertrouwensdiensten.

Onderdeel L, artikel 18.2a

Met het voorstel tot toevoeging van een tweede lid aan dit artikel wordt uitvoering gegeven aan artikel 17, eerste lid, van de eidas-verordening. Op grond daarvan moeten lidstaten een toezichthoudend orgaan aanwijzen en op grond van dit artikellid is dat de Minister van Economische Zaken. De taken van het toezichthoudend orgaan omvatten ingevolge de verordening onder meer het houden van toezicht op de naleving van voorschriften waaraan verleners van vertrouwensdiensten en hun vertrouwensdiensten moeten voldoen. Met dit toezicht op de naleving zijn op grond van het wetsvoorstel de door de Minister aangewezen ambtenaren belast. Die aangewezen ambtenaren zijn tevens belast met het verlenen van bijstand en bevoegd om deel te nemen aan een gezamenlijk onderzoek met andere toezichthoudende organen onder de daaraan in het wetsvoorstel gestelde voorwaarden. Het voornemen is dat de Minister ambtenaren van Agentschap Telecom hiermee zal belasten. Ditzelfde geldt voor het opstellen en bijhouden van de vertrouwenslijst, het behandelen van aanvragen tot het verleend krijgen van de status gekwalificeerd dan wel het beëindigen van die status en het in ontvangst nemen en behandelen van meldingen van veiligheidsincidenten. Op grond van de verordening dient een melding van een veiligheidsincident niet enkel aan het toezichthoudend orgaan plaats te vinden maar daarnaast, waar passend, ook aan de gegevensbeschermingsautoriteit en het bevoegde nationale orgaan voor informatieveiligheid, bedoeld in artikel 19, tweede lid, van de eidas-verordening. Daardoor kan het vereist zijn dat eenzelfde incident aan drie organen gemeld moet worden: aan de Minister van Economische Zaken die in dit onderdeel als het toezichthoudend orgaan, bedoeld in artikel 17, eerste lid, is aangemerkt en die het voornemen heeft ambtenaren van Agentschap Telecom met de uitvoering daarvan te belasten, aan het Cbp voor zover het een inbreuk op de veiligheid of het verlies van integriteit van persoonsgegevens betreft en die in onderdeel I van dit wetsvoorstel tot wijziging van hoofdstuk 11 van de Tw over bescherming van persoonsgegevens als gegevensbeschermingsautoriteit is aangemerkt, en aan de Minister van Veiligheid en Justitie (ingevolge de huidige portefeuilleverdeling de Staatssecretaris), die verantwoordelijk is voor het NCSC, en die in het voorgestelde derde lid als het bevoegde nationale orgaan voor informatieveiligheid, bedoeld in de verordening is aangemerkt.

Onderdeel M, artikel 18.3

Een verlener kan verplicht zijn op grond van de verordening een incident zowel aan AT, NCSC of ook aan het Cbp te moeten melden. In paragraaf 5.4 van het algemeen deel is het belang van samenhang

in meldingen en het vervolg daarop geadresseerd. Een inbreuk op of verlies van integriteit kan tot een verplichte melding aan zowel AT als NCSC leiden. Indien hierbij persoonsgegevens worden aangetast, kan tevens een verplichte melding aan het Cbp vereist zijn. Het in artikel 18.3 voorgestelde vierde lid, bevat de verplichting voor AT, NCSC en Cbp een samenwerkingsprotocol te sluiten in het belang van effectieve en efficiënte meldingen op grond van de verordening. Dit is te onderscheiden van het toezicht dat op basis van een melding plaatsvindt door AT en het Cbp. Het daarover te sluiten samenwerkingsprotocol is onderwerp van het vijfde lid. Het kan hierbij bijvoorbeeld gaan over het voeren van onderling overleg over de uitoefening van bevoegdheden.

Onderdeel N, artikel 18.3a en onderdeel O, artikel 18.7

De verstrekking van gegevens door andere bestuursorganen dan de ACM aan de Minister van Economische Zaken is in de voorgestelde wijziging ook toegestaan indien dit noodzakelijk is voor de uitvoering van en het toezicht op de eidas-verordening (onderdeel L). En voorts is het vorderen van inlichtingen ook toegestaan voor een juiste uitvoering van de verordening (onderdeel O).

Onderdeel P, artikel 18.15

Voor veel van rechtstreeks werkende eisen geldt dat de Europese Commissie de bevoegdheid heeft door middel van uitvoeringshandelingen referentienormen vast te stellen op basis van de comitologie-procedure. Indien aan een dergelijke norm, bijvoorbeeld een Europese vastgestelde technische norm, is voldaan, wordt aangenomen dat er overeenstemming is met de daarop betrekking hebbende eis die in de verordening staat vermeld. Het vaststellen van een norm sluit niet uit dat ook op andere wijze dan met inachtneming van die norm aan een eis uit de verordening kan worden voldaan.

De Europese Commissie is niet verplicht uitvoering te geven aan de vaststelling van referentienormen in alle gevallen waarvoor die bevoegdheid bestaat. Bij de voorbereiding van dit wetsvoorstel is onduidelijk in hoeverre op alle onderdelen waar dit nodig is (tijdig) referentienormen vastgesteld zullen worden. Voor het waarborgen van de betrouwbaarheid en de rechtszekerheid is evenwel noodzakelijk dat bij de toepasselijkheid van de verordening vanaf 1 juli 2016 in voldoende mate is voorzien in dergelijke technische normen. Gelet hierop biedt het voorgestelde artikel de mogelijkheid dit bij of krachtens algemene maatregel van bestuur te doen, voor zover dit voor een goede uitvoering van de eidas-verordening is vereist.

De Europese Commissie is voorts bevoegd referentienormen vast te stellen voor de accreditering van conformiteitsbeoordelingsinstanties, auditregels en het conformiteitsbeoordelingsverslag (artikel 20, vierde lid, van de eidas-verordening). Indien aan deze referentienormen wordt voldaan verbindt de verordening hier niet het vermoeden aan dat aan eisen uit de eidas-verordening is voldaan. Dit verschil met de andere referentienormen, zoals die onder meer in de artikelen 34, tweede lid, 38, zesde lid, 42, tweede lid, 44, tweede lid, 45, tweede lid, heeft tot gevolg dat het stellen van regels over deze referentienormen zich niet goed leent voor vastlegging in een algemeen verbindend voorschrift. De referentienormen voor accreditering en audits zijn niet meer en ook niet minder dan een richtlijn bij de beoordeling van conformiteitsbeoordelingsverslagen. Indien de Europese Commissie dergelijke referentienormen niet vaststelt, kan de Minister van Economische Zaken (Agentschap Telecom) als dat voor een goede uitvoering van de verordening noodzakelijk is overwegen hieromtrent beleidsregels of richtsnoeren vast te stellen.

Onderdeel Q, artikel 18.15a

De Europese Commissie kan uitvoeringshandelingen betreffende formaten en procedures met rechtstreekse werking vaststellen voor doeleinden van de meldplicht bij inbreuken op de veiligheid van vertrouwensdiensten (artikel 19, vierde lid, van de verordening). Dit kunnen ook formulieren zijn met een algemene of specifieke duiding van de bij een melding over te leggen gegevens. Daarbij kan die aanduiding zowel gelden voor een melding aan het toezichthoudend orgaan, het nationale orgaan voor informatieveiligheid, de gegevensbeschermingsautoriteit als de natuurlijke persoon of rechtspersoon die van een inbreuk of integriteitsverlies negatieve gevolgen ondervindt. Indien of zolang de Europese Commissie niet of eventueel in onvoldoende mate voorziet in een duiding van de bij een melding over te leggen gegevens, kunnen op grond van het voorgestelde artikel 18.15a voor een goede uitvoering van de verordening bij algemene maatregel van bestuur hierover regels worden gesteld voor een melding aan AT, NCSC en, voor zover het persoonsgegevens betreft, het Cbp, alsmede aan degene aan wie een vertrouwensdienst is verleend die naar verwachting ongunstige gevolgen ondervindt van een inbreuk die op grond van de verordening aan die organen moet worden gemeld. Bij de op grond van een algemene maatregel van bestuur te melden gegevens kan worden gedacht aan maatregelen die de aanbieder voorstelt of heeft getroffen om de inbreuk aan te pakken, de aard van de inbreuk of het verlies, vermoedelijke tijdstip van de aanvang van de inbreuk of het verlies en de mogelijke gevolgen en instanties waar meer informatie over de inbreuk kan worden

verkregen. Daarmee blijft er ruimte om in het geval dat noodzakelijk mocht zijn de te overleggen gegevens in nationale regelgeving vast te stellen. Uiteraard zal de Minister van Economische Zaken dit in voorkomend geval in overeenstemming met de Staatssecretaris van Veiligheid en Justitie doen. De aan AT, NCSC en Cbp te melden gegevens kunnen op die wijze waar mogelijk onderling afgestemd worden vastgelegd.

Onderdeel Q, artikel 18.15b

Voorafgaand aan afgifte van een gekwalificeerd certificaat is identiteitsverificatie met daartoe geschikte middelen verplicht. Dit dient overeenkomstig de nationale wetgeving plaats te vinden (artikel 24, eerste lid, eerste alinea, van de eidas-verordening). Identiteitsverificatie kan betrekking hebben op een natuurlijke persoon of op een natuurlijke persoon die een rechtspersoon vertegenwoordigt. In het laatste geval is het de bedoeling een gekwalificeerd certificaat dat daarvoor geschikt is op naam van een rechtspersoon te stellen. Rechtspersonen zijn in de zin van het VWEU alle entiteiten die zijn opgericht naar of worden beheerst door het recht van een lidstaat, ongeacht hun rechtsvorm. Voor Nederland worden voor de toepassing van de verordening hiertoe de rechtspersonen als bedoeld in de artikelen 1 tot en met 3 van Boek 2 van het Burgerlijk Wetboek gerekend en de zogenoemde Europese vennootschappen.

De verordening somt limitatief enkele manieren op die voor identiteitsverificatie van een natuurlijke persoon of rechtspersoon geschikt zijn. Identificatie in fysieke aanwezigheid is er daar één van. Dit is onderwerp van artikel 18.15b, zoals uit het eerste lid blijkt waarin wordt verwezen naar het voorschrift in de verordening dat op fysieke identificatie betrekking heeft. Indien een certificaat op naam van een natuurlijke persoon wordt gesteld, volgt uit het tweede lid met welke bescheiden de identiteit van die persoon in zijn fysieke aanwezigheid moet worden vastgesteld. Dit dient een in artikel 1 van de Wet op de identificatieplicht aangewezen geldig document te zijn. Bij rechtspersonen heeft identificatie in fysieke aanwezigheid betrekking op natuurlijke personen die vertegenwoordigingsbevoegd zijn. Dit is onderwerp van het derde tot en met zesde lid. De meest voorkomende situatie zal zijn dat een natuurlijk persoon bevoegd is een rechtspersoon te vertegenwoordigen bij de aanschaf van een op naam van die rechtspersoon te stellen gekwalificeerd certificaat. Identificatie omvat dan zowel identificatie van de natuurlijke persoon als identificatie van de rechtspersoon en de bevoegdheid tot vertegenwoordiging door de natuurlijke persoon van die rechtspersoon. De vertegenwoordigingsbevoegdheid van de natuurlijke persoon van wie in fysieke aanwezigheid de identiteit is vastgesteld, dient te worden gecontroleerd aan de hand van de gegevens in het handelsregister. In plaats daarvan kan ook de identiteit van een natuurlijke persoon worden vastgesteld die over een volmacht beschikt van een bestuurder van de rechtspersoon die over een in het handelsregister vastgelegde vertegenwoordigingsbevoegdheid beschikt. In dat geval hoeft die bestuurder niet in persoon te verschijnen, maar dient aan de hand van de gegevens in het handelsregister te worden vastgesteld dat de bestuurder die de volmacht heeft verleend vertegenwoordigingsbevoegd is. Dit vereist dat met een hoge mate van betrouwbaarheid wordt vastgesteld dat die bestuurder inderdaad degene is geweest die de volmacht heeft ondertekend. De gevolmachtigde natuurlijke persoon vervangt immers de fysieke aanwezigheid van de bestuurder als natuurlijke persoon bij identificatie. Gelet hierop wordt in het derde lid, onderdeel c, bepaald dat een volmacht met een gekwalificeerde elektronische handtekening of een door een notaris gelegaliseerde handtekening ondertekend dient te zijn. Het vierde lid heeft betrekking op vertegenwoordiging via een of meer tussenliggende rechtspersonen. De natuurlijke rechtspersoon vertegenwoordigt in dat geval een rechtspersoon, die weer de rechtspersoon vertegenwoordigt op wie de tenaamstelling betrekking heeft. En hierbij kan zelfs sprake zijn van een keten aan tussenliggende rechtspersonen, zoals bij concerns met achterliggende dochtermaatschappijen. In dat soort situaties dient een verificatie van de gehele keten ononderbroken terug te voeren zijn op de natuurlijke persoon van wie in fysieke aanwezigheid de identiteit wordt vastgesteld, en wel op dezelfde wijze met behulp van het handelsregister als bij rechtstreekse vertegenwoordiging. Afgezien van vertegenwoordiging van rechtspersonen kan het zich voordoen dat de natuurlijke persoon bijvoorbeeld een vennootschap onder firma vertegenwoordigt en voor die vennootschap bevoegd is de rechtspersoon te vertegenwoordigen op naam van wie het certificaat wordt gesteld. Uit het vijfde lid volgt dat ten aanzien van identificatie dan hetzelfde geldt als voor rechtspersonen.

Het zesde lid houdt rekening met rechtspersonen en met als zelfstandige eenheid naar buiten werkende samenwerkingsverbanden die niet in het Nederlandse handelsregister staan ingeschreven. Voor verificatie van gegevens kan in dat geval worden afgegaan op een buitenlandse register waarin de entiteit of eenheid staat ingeschreven dat soortgelijk is aan het handelsregister. Een register is voor de toepassing van het zesde lid soortgelijk aan het handelsregister in Nederland, indien de entiteit of eenheid is ingeschreven in een openbaar toegankelijk register dat in de betrokken staat een wettelijke grondslag heeft. Niet bepalend is of het register door een publiek- of privaatrechtelijke entiteit wordt beheerd. Indien er meerdere wettelijk geregelde en openbaar toegankelijke registers in een staat zijn, is bepalend het register dat het meest soortgelijk is aan het handelsregister ten aanzien van de echtheid en juistheid van de daarin aanwezige gegevens.

Onderdeel Q, artikel 18.15c

De eidas-verordening somt drie mogelijkheden op voor identificatie die elektronisch en/of op afstand kan worden uitgevoerd voorafgaand aan de afgifte van een gekwalificeerd certificaat.

De eerste mogelijkheid is dat identificatie op afstand plaatsvindt door middel van een geldig elektronisch identificatiemiddel met het betrouwbaarheidsniveau substantieel of hoog als bedoeld in de verordening. Bij het gebruik van dit identificatiemiddel is geen fysieke aanwezigheid vereist, maar vereist is in dat geval dat ten tijde van de uitgifte van dat middel identificatie in fysieke aanwezigheid wel heeft plaatsgevonden (artikel 24, eerste lid, onder b, van de verordening). Verificatie aan de hand van een elektronisch identificatiemiddel dat aan de daarin in de verordening gestelde eisen voldoet, vindt overeenkomstig nationale wetgeving plaats. Gelet hierop is in het eerste lid bepaald dat afgifte van een dergelijk middel met inachtneming van de aan identificatie of vertegenwoordiging gestelde eisen, bedoeld in artikel 18.15b moet zijn uitgegeven.

De tweede mogelijkheid voor elektronische identificatie voorafgaand aan de afgifte van een gekwalificeerd certificaat, bestaat uit verificatie van de identiteit aan de hand van een eerder afgegeven, geldig gekwalificeerd certificaat (artikel 24, eerste lid, onderdeel c, van de verordening). Het kan gaan om certificaten voor de gekwalificeerde elektronische handtekening (natuurlijke personen) of voor het gekwalificeerde elektronisch zegel (rechtspersonen). Identificatie met behulp van een dergelijk eerder afgegeven certificaat is alleen toegestaan, indien dat eerdere certificaat ofwel in fysieke aanwezigheid is afgegeven ofwel met een elektronisch identificatiemiddel dat voldoet aan de eisen die hiervoor bij de eerste mogelijkheid zijn genoemd. Het tweede lid bevestigt dat voorwaarde hierbij is dat afgifte van die identificatiemiddelen met inachtneming van respectievelijk overeenkomstig artikel 18.15b, heeft plaatsgevonden.

De derde mogelijkheid voor elektronische identificatie op afstand bij een afgifte van een gekwalificeerd certificaat is voor lidstaten optioneel (artikel 24, eerste lid, onderdeel d, van de verordening). Lidstaten kunnen er voor kiezen andere op nationaal niveau erkende identificatiemethoden die een mate van betrouwbaarheid verschaffen die gelijkwaardig is als fysieke aanwezigheid te accepteren als alternatief voor identificatie in fysieke aanwezigheid. Hierbij zou bijvoorbeeld wellicht kunnen worden gedacht aan identificatie met behulp van beeldverbindingen, die voldoende zekerheid bieden dat een persoon daadwerkelijk live in beeld is en zijn identiteit met voldoende zekerheid aan de hand van authentieke documenten kan worden vastgesteld. Hierbij geldt als eis dat het gelijkwaardige betrouwbaarheidsniveau door een conformiteitsbeoordelingsinstantie bevestigd dient te zijn. Gelet op het uitgangspunt van minimumomzetting van de verordening, is in het voorstel er vanaf gezien deze mogelijkheid nader te onderzoeken.

Onderdeel Q, artikel 18.15d

De gegevens die in een gekwalificeerd certificaat vermeld moeten staan, zijn in enkele bijlagen van de verordening voorgeschreven. Dit is een set aan basisgegevens die onverlet laat dat in een dergelijk certificaat eventueel ook andere, facultatieve, gegevens kunnen staan die gekoppeld zijn aan degene die het certificaat identificeert. Een voorbeeld hiervan zijn gegevens die bevestigen dat een persoon bevoegd is een ander te vertegenwoordigen, zoals bij een certificaat voor een elektronische handtekening waaruit tevens de bevoegdheid tot wettelijke vertegenwoordiging, volmacht of lastgeving blijkt. Deze aan een persoon gekoppelde aanvullende gegevens worden attributen genoemd. Bij natuurlijke personen betreft dit naar hun aard persoonsgegevens. Ook de inhoud van specifieke attributen moeten op grond van de verordening op juistheid worden geverifieerd overeenkomstig de nationale wetgeving. Doordat attributen in beginsel op allerlei gegevens betrekking kunnen hebben, is het niet goed mogelijk een procedure voor te schrijven op basis waarvan verificatie van al die gegevens ongeacht de achtergrond daarvan, kan plaatsvinden. Dit zal per geval verschillen, zodat als algemene eis geldt dat verificatie op een niveau plaatsvindt dat past bij de betrouwbaarheid die aan de status gekwalificeerd wordt toegekend. Een attribuut kan bijvoorbeeld betrekking hebben op gegevens die aangeven dat de certificaathouder gemachtigd is een ander te vertegenwoordigen. Dit vereist dat niet alleen de identiteit van de certificaathouder is vastgesteld, maar tevens van de vertegenwoordigde en zijn bevoegdheid tot vertegenwoordiging. De dienstverlener kan dit vaststellen met behulp van een volmacht die is ondertekend door de vertegenwoordigde met een gekwalificeerde elektronische handtekening als bedoeld in artikel 3, onder 12, van de eidas-verordening of met een door een notaris gelegaliseerde handtekening. Ook is denkbaar dat de vertegenwoordigde de volmacht bij de vertrouwensdienstverlener in fysieke aanwezigheid ondertekent na voorafgaande identiteitsvaststelling aan de hand van een in artikel 1 van de Wet op de identificatieplicht aangewezen geldig document. Dit is een passende verificatie van deze specifieke attributen in de zin van het voorgestelde artikel.

Onderdeel Q, artikel 18.15e

Een certificaat kan een gefingeerde naam bevatten in plaats van te zijn gesteld op de echte naam van een natuurlijke persoon. De houder van het certificaat maakt gebruik van een pseudoniem. De verordening voorziet evenals onder de Richtlijn elektronische handtekening in de mogelijkheid van het gebruik van een pseudoniem bij een gekwalificeerd certificaat voor elektronische handtekeningen. Ook bij een gekwalificeerd certificaat voor website-authenticatie kan van een pseudoniem gebruik worden gemaakt. Op grond van de verordening moet in een certificaat vermeld worden als de naamgeving een pseudoniem betreft. Degene die op een dergelijk certificaat vertrouwt als ontvanger ervan, kan in dat geval door controle van het certificaat nagaan dat het een pseudoniem betreft. De vertrouwende partij weet dat het om een gefingeerde naam gaat, maar weet ook dat de identiteit van de achterliggende persoon onzichtbaar is geverifieerd door de verlener van vertrouwensdiensten. Hij krijgt de bevestiging dat het certificaat afkomstig is van een bepaalde echt bestaande persoon. Het gebruik van pseudoniemen kan een instrument zijn ter bescherming van persoonsgegevens in het kader van ‘privacy by design’ of dataminimalisatie. De vertrouwende partij weet niet wie er achter het pseudoniem zit en hoeft dat bij sommige transacties ook niet te weten.

Onderdeel R, artikelen 18.16 en 18.16a

Op grond van de huidige Telecommunicatiewet is de Minister van Economische Zaken bevoegd een of meer organisaties aan te wijzen die bevoegd zijn certificatiedienstverleners te toetsen op overeenstemming met de bij en krachtens deze wet gestelde eisen en daartoe een bewijs van toetsing af te geven. Het door de minister kunnen aanwijzen van certificeringsorganisaties vervalt in het wetsvoorstel (artikel 18.16, van de Tw). De verordening stelt zelf eisen aan instanties die deze verleners en hun diensten moeten toetsen. Deze instanties worden conformiteitsbeoordelingsinstanties genoemd. Conformiteitsbeoordelingsinstanties moeten geaccrediteerd zijn in overeenstemming met de accreditatieverordening om een conformiteitsbeoordeling te verrichten van een gekwalificeerde verlener van vertrouwensdiensten en van de door hem verleende vertrouwensdiensten (artikel 3, onder 18, van de verordening). Over de accreditering, toe te passen auditregels en verslagen van die instanties kan de Europese Commissie referentienormen vaststellen. Voor Nederland is de instantie die bevoegd is tot accreditatie de Raad voor Accreditatie.
Voorts vervalt in het wetsvoorstel de toekenning van een wettelijk vermoeden als bedoeld in artikel 18.16a. De verordening voorziet hierin niet en dit wordt ook niet wenselijk geacht (zie verder paragraaf 5.6 van het algemeen deel van deze toelichting).

Onderdeel S, artikel 18.17

De bewoordingen in dit artikel zijn aangepast aan de in de eidas-verordening gebruikte begrippen. Onder de richtlijn elektronische handtekeningen werd het gebruik van een veilig middel voor elektronische handtekeningen geregeld. In de verordening is het begrip veilig middel vervangen door gekwalificeerd middel, waarbij dit ook betrekking kan hebben op een elektronisch zegel.

Onderdeel T, artikel 18.17a

Bij het aanmaken van een elektronische handtekening kan gebruik worden gemaakt van een gekwalificeerd middel. De instellingen die een aanbieder van een middel mogen certificeren om het als gekwalificeerd middel te mogen aanbieden, moeten door de lidstaten worden aangewezen. Die aanwijzing mag zowel op openbare als private organen betrekking hebben. De Europese Commissie is bevoegd gedelegeerde handelingen vast te stellen met betrekking tot het opstellen van specifieke criteria waaraan die organen moeten voldoen (artikel 30, eerste en vierde lid, van de eidas-verordening).

Deze in de verordening gevolgde benadering sluit goeddeels aan bij de wijze waarop dit in de huidige Telecommunicatiewet is geregeld. Op grond van artikel 18.17a, eerste lid, is de Minister bevoegd een of meer instellingen aan te wijzen die zijn belast met het beoordelen van de overeenstemming van een veilig middel voor het aanmaken van elektronische handtekeningen met de eisen bedoeld in artikel 18.17 en het daartoe afgeven van verklaringen. Als gevolg van de verordening wordt de werking van dit artikel verbreed tot gekwalificeerde middelen voor het aanmaken van elektronische handtekeningen en elektronische zegels. Daarnaast mogen ook in de nieuwe situatie bij of krachtens algemene maatregel van bestuur regels worden gesteld over de eisen waaraan instellingen moeten voldoen om voor een aanwijzing door de Minister in aanmerking te komen. Daar wordt evenwel in het tweede lid aan toegevoegd dat dit niet kan als de Europese Commissie specifieke criteria vaststelt waaraan door de lidstaten aangewezen organen moeten voldoen. In dat geval wordt dan op basis van de verordening met rechtstreekse werking al voorzien in die eisen.

De door de Minister aangewezen organen die bevoegd zijn verleners van middelen te certificeren,

moeten hun certificering baseren op een veiligheidsbeoordeling uitgevoerd in overeenstemming met door de Europese Commissie vastgestelde normen inzake de veiligheidsbeoordeling van producten op het gebied van informatietechnologie. Die normen zijn in een door de Commissie vastgestelde lijst opgenomen. In plaats van de veiligheidsbeoordeling uit te voeren aan de hand van die vastgestelde normen, mag een gecertificeerde instelling dit ook doen op basis van een ander proces. Voorwaarde daarbij is dat er geen vastgestelde normen zijn of wanneer een veiligheidsbeoordeling op grond van vastgestelde normen gaande is. Verder dient dit proces vergelijkbare beveiligingsniveaus te hanteren en de gecertificeerde instelling de Commissie van dat andere proces op de hoogte stellen.

De door de Minister aangewezen certificeringsinstellingen zijn op grond van het nieuw ingevoegde zesde lid gehouden binnen twee weken nadat een veiligheidsbeoordeling resulteert in een positief oordeel de Minister daarover te informeren. En ingevolge het zevende lid kunnen over de daartoe te verstrekken gegevens en wijze van verstrekking bij of krachtens algemene maatregel van bestuur regels worden gesteld. Deze informatieverplichting is noodzakelijk om de Minister in staat te stellen te voldoen aan verplichtingen tot informatieverstrekking aan de Europese Commissie over gekwalificeerde middelen voor het aanmaken van elektronische handtekeningen en elektronische zegels. Over de inhoud van die informatieverplichtingen kan de Commissie op basis van uitvoeringshandelingen formaten en procedures vaststellen. De ontvangen informatie gebruikt de Commissie voor het opstellen van een lijst van gecertificeerde gekwalificeerde middelen als aangeduid. Deze lijst publiceert de Commissie en wordt bijgehouden (artikel 31 en 39, derde lid, van de eidas-verordening)

Onderdeel U, artikel 18.18

Hoofdstuk III van de verordening bevat allerlei eisen waaraan verleners van vertrouwensdiensten verplicht zijn te voldoen. Het wetsvoorstel bepaalt dat door de Minister aangewezen ambtenaren met het toezicht hierop belast zijn. Tegen verleners van vertrouwensdiensten die zich niet aan deze bepalingen uit de verordening houden kunnen bestuurlijke maatregelen worden getroffen. Ter verduidelijking dat handhaving zich ook uitstrekt tot de naleving van deze eisen uit de eidas-verordening, bepaalt het eerste lid uitdrukkelijk dat het verleners van vertrouwensdiensten verboden is in strijd te handelen met hoofdstuk III, van de eidas-verordening. Het tweede lid is tevens van toepassing op een verlener van gekwalificeerde vertrouwensdiensten waarvan de status gekwalificeerd is beëindigd. Die verlener zal dan wederom de gehele procedure voor de toekenning van de status gekwalificeerd met succes dienen te doorlopen. Dit omvat daarmee verleners van vertrouwensdiensten die hun diensten als gekwalificeerd aanbieden, terwijl zij niet of niet langer over de status gekwalificeerd beschikken voor henzelf en voor hun diensten. Tegen verleners van vertrouwensdiensten die moedwillig zich als gekwalificeerd presenteren of hun vertrouwensdiensten als zodanig aanbieden kunnen derhalve bestuurlijke maatregelen worden getroffen, zoals het opleggen van een boete. Er is vanaf gezien de mogelijkheid van strafrechtelijk sanctioneren op grond van de Wet op de economische delicten met dit wetsvoorstel te herintroduceren. In het kader van de Instellingswet Autoriteit Consument en Markt is afgezien van de mogelijkheid van strafrechtelijke handhaving naast bestuursrechtelijke handhaving door ACM. Dit heeft bij de invoering van die wet geleid tot het schrappen van enkele verwijzingen in de Wet op de Economische Delicten die betrekking hadden op onder meer de eisen die gesteld worden aan het mogen aanbieden van gekwalificeerde certificaten. In dit wetsvoorstel berust het toezicht op het verlenen van vertrouwensdiensten niet bij ACM maar bij de Minister. Dit enkele verschil heeft in dit geval niet geleid tot het alsnog herintroduceren in het wetsvoorstel van strafrechtelijke handhaving ten aanzien van gekwalificeerde vertrouwensdiensten. Daarbij is meegewogen dat anders dan onder de huidige Telecommunicatiewet het toezicht zich tevens, zij het beperkt, uitstrekt tot niet-gekwalificeerde verleners van vertrouwensdiensten. Bevoegdheden zoals het vorderen van inlichtingen (artikel 18.7) of het opvragen daarvan bij andere bestuursorganen in het kader van toezicht (artikel 18.3a) strekken zich ten principale ook uit tot verleners van niet-gekwalificeerde vertrouwensdiensten die zich ten onrechte voordoen als gekwalificeerde verleners.

Onderdeel V, artikel 18.22

In dit onderdeel wordt geregeld dat de eidas-verordening kenbaar is te raadplegen via de in de Staatscourant opgegeven vindplaats.

Onderdeel W, artikel 20.15a

Door de voorgestelde wijziging in het toezicht zal de verantwoordelijkheid voor verschillende activiteiten, waaronder het toezicht overgaan van ACM op door de Minister aangewezen ambtenaren (Agentschap Telecom). Dit artikel bevat overgangsrecht ten aanzien van aanvragen, samenwerkingsprotocollen, archiefbescheiden en gegevens uit het register over aanbieders van gekwalificeerde certificaten en hun diensten. Het overgangsrecht beperkt zich ingevolge het eerste lid uitsluitend tot hetgeen betrekking heeft op certificatiedienstverleners of gekwalificeerde certificaten. Van de

overgang van activiteiten naar het AT is te onderscheiden het toepasselijk recht bij de overgang op aanvragen en de behandeling van bezwaar en beroep dat onderwerp is van artikel XI.

Onderdeel X, artikel 20.16

Het bestaande artikel 20.16 voorziet in voorschriften betreffende de verstrekking van gegevens ten behoeve van de registratie van certificatiedienstverleners, waarbij tevens verschillende situaties inzake overgangsrecht worden onderscheiden. Doordat de registratie op de vertrouwenslijst met rechtstreekse werking is geregeld in de verordening en bestaande certificatiedienstverleners ingevolge artikel 51, derde lid, van de verordening worden aangemerkt als gekwalificeerde verleners van vertrouwensdiensten, zullen reeds geregistreerde certificatiedienstverleners op de door Agentschap Telecom op te stellen en bij te houden vertrouwenslijst geregistreerd worden als gekwalificeerde verleners van vertrouwensdiensten voor gekwalificeerde certificaten voor elektronische handtekeningen. Artikel 20.16 vervalt in het wetsvoorstel.

Onderdeel Y, artikel 20.15a

Dit onderdeel betreft een verbetering van een technische omissie.

Artikel II (artikelen 3:15a tot en met 15c BW)

De artikelen 3:15a tot en met c BW betreffen de implementatie van enkele bepalingen uit de Richtlijn elektronische handtekeningen. Artikel 3:15a geeft regels met betrekking tot de elektronische handtekening en bepaalt onder meer de voorwaarden voor het bestaan van rechtsgevolgen van elektronische handtekeningen en bevat definities. Artikel 3:15b BW bevat een regeling voor de erkenning van gekwalificeerde certificaten die buiten de Europese Gemeenschappen (hierna verder: EG) en Europese Economische Ruimte (hierna verder: EER) zijn afgegeven. Ingevolge artikel 3:15c BW zijn buiten het vermogensrecht de bepalingen van de artikelen 3:15a en 3:15b BW van overeenkomstige toepassing, voor zover de aard van de rechtshandeling of van de rechtsbetrekking zich daartegen niet verzet.

De intrekking van de richtlijn door de verordening en het geven van eigen regels op het terrein van de elektronische handtekening betekent dat de artikelen ter implementatie van de richtlijn dienen te vervallen. De verordening onderscheidt een elektronische handtekening, een geavanceerde elektronische handtekening en een gekwalificeerde elektronische handtekening. Een elektronische handtekening is in de verordening gedefinieerd als gegevens in elektronische vorm die gehecht zijn aan of logisch verbonden zijn met andere gegevens in elektronische vorm en die door de ondertekenaar worden gebruikt om te ondertekenen (artikel 3, onder 10, van de verordening). Een geavanceerde elektronische handtekening is ingevolge artikel 3, onderdeel 11, een elektronische handtekening die voldoet aan de eisen van artikel 26. Dit houdt in dat de handtekening dient te voldoen aan de volgende eisen:
a) zij is op unieke wijze aan de ondertekenaar verbonden;
b) zij maakt het mogelijk de ondertekenaar te identificeren;
c) zij komt tot stand met gegevens voor het aanmaken van elektronische handtekeningen die de ondertekenaar, met een hoog vertrouwensniveau, onder zijn uitsluitend controle kan gebruiken,
d) zij is op zodanige wijze aan de daarmee ondertekende gegevens verbonden, dat elke wijziging achteraf van de gegevens kan worden opgespoord.

Een gekwalificeerde elektronische handtekening is een geavanceerde elektronische handtekening die is aangemaakt met een gekwalificeerd middel voor het aan maken van elektronische handtekeningen en die gebaseerd is op een gekwalificeerd certificaat voor elektronische handtekeningen (art. 3, onderdeel 12).
Zoals in het algemeen deel van de toelichting is aangegeven, bepaalt de verordening dat een gekwalificeerde elektronische handtekening hetzelfde rechtsgevolg heeft als een handgeschreven handtekening. De rechtsgevolgen van de overige handtekeningen zijn ter bepaling aan de lidstaten (zie paragraaf 6.1 en 6.2 van het algemeen deel). Voor de geavanceerde elektronische handtekening en enig andere gewone elektronische handtekening zijn de rechtsgevolgen in artikel 3:15a BW (nieuw) opgenomen. Hiervoor is aangesloten bij het huidige eerste lid van artikel 15a. Een geavanceerde elektronische handtekening als bedoeld in onderdeel 11, en een andere elektronische handtekening als bedoeld in onderdeel 10, van artikel 3 van de verordening hebben dezelfde rechtsgevolgen als een geschreven handtekening, indien de methode voor ondertekening die gebruikt is voldoende betrouwbaar is, gelet op het doel waarvoor de elektronische handtekening is gebruikt en op alle overige omstandigheden van het geval.

Het tweede lid van het huidige artikel 3:15a BW inzake het vermoeden van het bestaan van een rechtsgevolg van de gekwalificeerde elektronische handtekening dient te worden geschrapt, nu de verordening zoals gezegd bepaalt dat de gekwalificeerde elektronische handtekening hetzelfde rechtsgevolg heeft als een handgeschreven handtekening. De overige leden 3 tot en met 5 van artikel

3:15a BW hebben evenmin bestaansrecht meer. Het derde lid bepaalt dat een methode die voor authentificatie wordt gebruikt niet enkel op de in dit lid aangegeven gronden als onvoldoende betrouwbaar kan worden aangemerkt. De verordening geeft in artikel 25, eerste lid, een eigen regeling op dit punt en bepaalt dat het rechtsgevolg van een elektronische handtekening en de toelaatbaarheid ervan als bewijsmiddel in gerechtelijke procedures niet mogen worden ontkend louter op grond van het feit dat de handtekening elektronisch is of niet aan de eisen voor gekwalificeerde handtekeningen voldoet.

Het vierde lid en vijfde lid van het huidige artikel 3:15a BW geven definities van de begrippen elektronische handtekening en ondertekenaar op grond van de richtlijn. De verordening geeft omschrijvingen van deze begrippen in artikel 3, onderdeel 10 en onderdeel 9. Het zesde lid bepaalt dat van de leden 2 en 3 kan worden afgeweken. Zoals hiervoor is aangegeven vervallen deze leden en dient derhalve ook het zesde lid te vervallen.

Artikel 3:15b BW noemt drie voorwaarden voor de erkenning van gekwalificeerde certificaten afgegeven aan het publiek door een certificatiedienstverlener gevestigd in een derde land. Certificaten worden gelijkgesteld aan gekwalificeerde certificaten die door een in de EG of EER gevestigde certificatiedienstverlener worden afgegeven indien a) de certificatiedienstverlener voldoet aan de eisen in de richtlijn en in het kader van een in een lidstaat van de EG of EER ingestelde vrijwillige-accreditatieregeling is geaccrediteerd, danwel b) een in de EG of EER gevestigde certificatiedienstverlener die voldoet aan de richtlijn in staat voor dit certificaat of c) het certificaat of de certificatiedienstverlener is erkend in het kader van een bilaterale of multilaterale overeenkomst tussen de EG of EER en derde landen of internationale organisatie. Zoals ook in paragraaf 5.11 en 5.12 is aangegeven, bevat de verordening in artikel 14 een eigen regeling inzake de verlening van vertrouwensdiensten door aanbieders uit derdelanden: erkenning vindt plaats op grond van een overeenkomst tussen de EU en een derdeland of internationale organisatie. Artikel 3:15b dient dan ook te vervallen.

Ingevolge artikel 3:15c BW vinden de artikelen van de betreffende afdeling (artikelen 15a en 15b) buiten het vermogensrecht van overeenkomstige toepassing, voor zover de aard van de rechtshandeling of van de rechtsbetrekking zich daartegen niet verzet. Het artikel ziet primair op privaatrechtelijke verhoudingen buiten de sfeer van het vermogensrecht, maar toepassing op andere rechtsgebieden is niet uitgesloten (Kamerstukken II 27 743 2001/01, nr. 3, blz. 11). Op verschillende plaatsen in de wetgeving wordt naar artikel 3:15a verwezen.
De regeling van de vertrouwensdiensten van de verordening strekt zich uit tot in beginsel alle domeinen. De regeling van de elektronische handtekening van de verordening geldt dan ook voor zowel het private als publieke domein. De voorgestelde bepaling in artikel 3:15a over de rechtsgevolgen voor de gewone en geavanceerde elektronische handtekening kan in beginsel eveneens van overeenkomstige toepassing worden verklaard voor andere rechtsgebieden buiten het vermogensrecht. In artikel 3:15c BW wordt daarom, op dezelfde voet als thans het geval is, bepaald dat artikel 3:15a BW buiten het vermogensrecht van overeenkomstige toepassing is.

Artikel III (artikel 6:196b BW)

Artikel 6:196b BW geeft een specifiek aansprakelijkheidsregime voor de certificatiedienstverlener die gekwalificeerde certificaten afgeeft aan het publiek. Met dit artikel is artikel 6 van de Richtlijn elektronische handtekening geïmplementeerd.
Doordat de verordening de Richtlijn elektronische handtekening intrekt, dient dit artikel ter implementatie van de richtlijn te vervallen. De verordening geeft in artikel 13 een eigen regeling voor aansprakelijkheid voor verleners van vertrouwensdiensten (zie paragraaf 5.9 en 5.10 van het algemeen deel van de toelichting).

Artikel IV (artikelen 7:655 en 932 BW)

Onderdeel A

Artikel 7:655 BW, derde lid, ziet op het verstrekken van een opgave door de werkgever aan de werknemer van elementen van de arbeidsovereenkomst. Wanneer dit elektronisch wordt gedaan, dient deze opgave te zijn voorzien van een handtekening die voldoet aan de eisen, bedoeld in artikel 3:15a, tweede lid, BW. Dit tweede lid bevat de onderdelen a tot en met f, dat wil zeggen de voorwaarden voor een gekwalificeerde elektronische handtekening. Het tweede lid van artikel 3:15a, dient te vervallen (zie paragraaf 6.2 van het algemeen deel en hiervoor bij artikel II). In artikel 3, onderdeel 12, van de verordening wordt de gekwalificeerde handtekening omschreven.
De verwijzing naar alle onderdelen van het tweede lid van artikel 3:15a BW dient derhalve te worden vervangen door een verwijzing naar artikel 3, onderdeel 12, van de verordening.

Onderdeel B

Artikel 7:932 BW ziet op het afgeven van een polis door de verzekeraar. Als dit een polis betreft die is opgemaakt op een wijze als bedoeld in artikel 156a lid 1 van het Wetboek van Burgerlijke Rechtsvordering (op elektronische wijze) moet de polis zijn voorzien van een elektronische handtekening die voldoet aan de eisen, bedoeld in het tweede lid van artikel 3:15a BW. Ook hier geldt dat met de inwerkingtreding van de verordening verwezen dient te worden naar de gekwalificeerde elektronische handtekening van artikel 3, onderdeel 12, van de verordening.

Artikel V (artikel 2:16 Awb)

Sinds de opname van Afdeling 2.3 van de Algemene wet bestuursrecht (hierna: Awb) over verkeer langs elektronische weg in de Awb, sluit de Awb wat betreft de elektronische handtekening aan bij het BW (Kamerstukken II 2001/02, 28 483, nr. 3, p. 18). Artikel 2:16 Awb strekt ertoe de elektronische handtekening gelijk te stellen met de handgeschreven handtekening, geeft een nadere uitwerking aan de betrouwbaarheid van de elektronische handtekening en maakt het mogelijk om aanvullende eisen te stellen bij wettelijk voorschrift. De mogelijkheid om nadere eisen te stellen volgde uit artikel 3, zevende lid, van de richtlijn inzake elektronische handtekeningen. De intrekking van de richtlijn door de verordening en de nieuwe regels over elektronische handtekeningen die de verordening geeft, nopen tot wijziging van artikel 2:16 Awb.

Het eerste lid stelt buiten twijfel dat aan het vereiste van ondertekening niet alleen kan worden voldaan door een handgeschreven handtekening, maar ook door een elektronische handtekening. De tekst van deze volzin is zoveel mogelijk ongewijzigd gebleven. Aangezien het begrip elektronische handtekening in de verordening anders is gedefinieerd dan in de richtlijn, is het woord ‘authentificatie’ vervangen door ‘ondertekening’. Hierdoor is het artikel in overeenstemming gebracht met de nieuwe definitie uit de verordening. Uit artikel 25, tweede en derde lid, van de verordening volgt dat een gekwalificeerde elektronische handtekening hetzelfde rechtsgevolg heeft als een handgeschreven handtekening. Een dergelijke handtekening die op een in een lidstaat afgegeven gekwalificeerd certificaat is gebaseerd, moet in alle lidstaten als een gekwalificeerde elektronische handtekening worden erkend (artikel 25, derde lid, verordening). De rechtsgevolgen van de andere elektronische handtekeningen dienen te worden vastgesteld door het nationale recht (zie overweging 49). Daartoe dient artikel 2:16, eerste lid, Awb. Ook geavanceerde en andere elektronische handtekeningen kunnen hetzelfde rechtsgevolg hebben als een handgeschreven handtekening, indien de methode voor ondertekening die gebruikt is, voldoende betrouwbaar is, gelet op de aard en inhoud van het elektronische bericht en het doel waarvoor het is gebruikt. Op grond van het eerste lid van artikel 25 van de Verordening mogen het rechtsgevolg van een elektronische handtekening en de toelaatbaarheid ervan als bewijsmiddel in gerechtelijke procedures, niet worden ontkend louter op grond van het feit dat de handtekening elektronisch is of niet aan de eisen voor gekwalificeerde elektronische handtekeningen voldoet. Voor geavanceerde en gewone elektronische handtekeningen geldt dat om te beoordelen of in een bepaald geval een elektronische handtekening voldoende betrouwbaar is, dient te worden gelet op de aard en de inhoud van het bericht en het doel waarvoor het wordt gebruikt. Indien gelet op deze omstandigheden sprake is van een voldoende betrouwbare handtekening, heeft deze hetzelfde rechtsgevolg als een handgeschreven handtekening en kan deze derhalve niet door een bestuursorgaan worden geweigerd.
Niet elke handtekening is in het licht van het doel waarvoor de elektronische gegevens worden gebruikt, de aard van de rechtsverhouding tussen de ondertekenaar en het bestuursorgaan of de overige omstandigheden van het geval geschikt om in aanmerking te komen voor juridische gelijkstelling met een handgeschreven handtekening. Daarom maakt het tweede lid het mogelijk dat het gebruik van een bepaald type elektronische handtekening door de centrale overheid bij of krachtens een wet of door een ander bestuursorgaan met regelgevende bevoegdheid in de eigen verordening wordt voorgeschreven (vgl. ook artikel 27, eerste en tweede lid, van de verordening). Het tweede lid vervangt de volzin in het artikel waarin werd bepaald dat bij wettelijk voorschrift aanvullende eisen kunnen worden gesteld. Deze volzin werd destijds opgenomen omdat dit uit de richtlijn volgde. Een vergelijkbare bepaling is niet teruggekomen in de verordening en de verdere uitwerking van de geavanceerde en gekwalificeerde elektronische handtekening in het betreffende uitvoeringsbesluit[1] is uitputtend, zodat lidstaten in hun nationale wetgeving geen nadere eisen aan dit type handtekeningen stellen. Daarom wordt de mogelijkheid daartoe in het tweede lid voor dit type handtekeningen geschrapt. Ingeval bij wettelijk voorschrift de gewone elektronische handtekening wordt voorgeschre-

[1] Uitvoeringsbesluit (EU) 2015/1506 van de Commissie van 8 september 2015 tot vaststelling van specificaties betreffende formaten van geavanceerde elektronische handtekeningen en geavanceerde zegels die door openbare instanties moeten worden erkend overeenkomstig respectievelijk artikel 27, lid 5, en artikel 37, lid 5, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt (PbEU 2015, L 235).

ven, is wel mogelijk hierbij aanvullende eisen te stellen. Met deze eisen kan de veiligheid en betrouwbaarheid van de ondertekening door middel van een gewone elektronische handtekening worden verzekerd. Zo kunnen bijvoorbeeld eisen worden gesteld aan het niveau van authenticatie op basis waarvan de elektronische handtekening wordt aangemaakt. Ook kunnen eisen worden gesteld aan de onafhankelijkheid en veiligheid van het mechanisme waarmee de gegevens die dienen ter ondertekening, aan het te ondertekenen document, bericht of de gestandaardiseerde gegevensset worden gehecht. Evenzo kunnen bijvoorbeeld aanvullende eisen worden gesteld aan de elektronische handtekening die door middel van een tablet wordt gezet. In dit verband kan hoofdstuk 9 over ondertekenen van de Handreiking voor overheidsorganisaties van het Forum Standaardisatie als leidraad dienen (Forum Standaardisatie, Betrouwbaarheidsniveaus voor authenticatie bij elektronische overheidsdiensten, versie 3, augustus 2014).

Wat betreft de verwijzing in artikel 2:16 Awb naar artikel 3:15a, tweede tot en met zesde lid, en artikel 3:15b BW wordt voorgesteld deze te laten vervallen omdat deze bepalingen in het BW eveneens vervallen. De verordening geeft eigen regels over de onderwerpen die in deze artikelen geregeld waren.

Volledigheidshalve wordt hier opgemerkt dat de nadere eisen die op grond van artikel 2:15, eerste lid, Awb kunnen worden gesteld aan het gebruik van de elektronische weg, geen betrekking kunnen hebben op elektronische handtekeningen. Tevens mag er, conform artikel 27, derde lid, van de verordening, voor grensoverschrijdend gebruik bij een door een openbare instantie aangeboden onlinedienst geen elektronische handtekening van een hoger betrouwbaarheidsniveau dan een gekwalificeerde elektronische handtekening worden vereist.

Artikel VI (artikel 1072b Wet boek van Burgerlijke Rechtsvordering)

In artikel 1072b is mogelijk gemaakt dat het arbitrale vonnis van artikel 1057, tweede lid, Rv ook kan worden opgemaakt in elektronische vorm door het te voorzien van een elektronische handtekening die voldoet aan het bepaalde in artikel 3:15a, eerste en tweede lid, BW. Er moet voldaan zijn aan de vereisten voor een gekwalificeerde elektronische handtekening. Daar artikel 3:15a, tweede lid, vervalt (zie paragraaf 6.2 van het algemeen deel en hiervoor bij artikel II) en de verordening in artikel 3, onderdeel 12, een omschrijving van de gekwalificeerde elektronische handtekening bevat, dient voortaan te worden verwezen naar dit artikel 3, onderdeel 12, van de verordening.

Artikelen VII tot en met IX (artikel 7e, Kadasterwet, artikel 8.2, Wet handhaving consumentenbescherming, artikel 35, vierde lid, Wet op de omzetbelasting 1968)

In artikel 7e, eerste lid, van de Kadasterwet, is bepaald dat indien in die wet wordt voorgeschreven dat een document van een elektronische handtekening wordt voorzien, een elektronische handtekening wordt gebruikt die voldoet aan de eisen, genoemd in artikel 15a, tweede lid, onderdelen a tot en met f, van Boek 3 van het Burgerlijk Wetboek. Steeds moet voldaan zijn aan de voorwaarden gesteld aan een elektronische gekwalificeerde handtekening. Artikel 3:15a, tweede lid, vervalt (zie paragraaf 6.2 van het algemene deel van de toelichting en hiervoor bij artikel II). Verwezen dient in dit artikel te worden naar artikel 3, onderdeel 12, van de verordening.

Het derde lid van artikel 7e van de Kadasterwet vervalt. Destijds volgde uit de richtlijn dat de lidstaten aanvullende eisen konden stellen aan de elektronische handtekening. Nu de richtlijn is ingetrokken en een vergelijkbare bepaling niet is teruggekomen in de verordening, dient de mogelijkheid om aanvullende eisen te stellen dan ook te vervallen.

In artikel 8.2, eerste lid, van de Wet handhaving consumentenbescherming is bepaald dat degene die een dienst van een informatiemaatschappij verleent als bedoeld in de artikelen 15d, eerste en tweede lid, van Boek 3 BW, de artikelen 15a tot en met 15c in acht dient te nemen. In dit lid wordt rekening gehouden met het vervallen van artikel 15b van Boek 3 van het Burgerlijk Wetboek (zie paragraaf 5.12 van het algemeen deel van de toelichting).

In het vierde lid van artikel 35b van de Wet op de omzetbelasting 1968 wordt aangegeven met welke technologieën de authenticiteit van de herkomst en de integriteit van de inhoud van een elektronische factuur kunnen worden gewaarborgd. In onderdeel a van dit lid wordt verwezen naar een geavanceerde handtekening van de Richtlijn elektronische handtekeningen die gebaseerd is op een gekwalificeerd certificaat en aangemaakt wordt met een veilig middel, derhalve naar een gekwalificeerde elektronische handtekening. Deze verwijzing dient vervangen te worden door een verwijzing naar de gekwalificeerde elektronische handtekening van de verordening.

Artikel X (artikel 34a Wet bescherming persoonsgegevens)

In het voorgestelde artikel worden verleners van vertrouwensdiensten grotendeels uitgezonderd van de meldplicht op grond van het artikel 34a van de Wet bescherming persoonsgegevens (Stb. 2015, 230, inwerkingtreding 1 januari 2016, zie Stb. 2015, 281). De meldplicht door verleners van vertrouwensdiensten aan het Cbp op basis van de verordening is in het wetsvoorstel door middel van een wijziging van de Telecommunicatiewet geregeld. Dit biedt de mogelijkheid specifiek rekening te houden met de rechtstreekse werking van de verordening ten aanzien van de norm op basis waarvan gemeld dient te worden, degenen aan wie gemeld dient te worden, en indien de Europese Commissie hiervoor uitvoeringshandelingen vaststelt ook de bij een melding over te leggen gegevens.

Artikel XI

Uit de huidige Telecommunicatiewet volgt dat ACM met inachtneming van het bepaalde bij en krachtens de Telecommunicatiewet bevoegd is een aanvraag tot registratie van een certificatiedienstverlener in behandeling te nemen en daarop een besluit te nemen. Die bevoegdheid blijft ongewijzigd gelden voor iedere aanvraag totdat dit wetsvoorstel tot wet is verheven en in werking is getreden, met dien verstande dat als op 1 juli 2016 het wetsvoorstel nog niet tot wet is verheven en in werking is getreden het bepaalde bij en krachtens de huidige Telecommunicatiewet met inachtneming van het bepaalde in de verordening geldt. Indien het wetsvoorstel tot wet is verheven en in werking is getreden en door ACM op een lopende aanvraag tot registratie van een certificatiedienstverlener op dat tijdstip nog geen besluit is genomen, bepaalt het wetsvoorstel dat de behandeling daarvan bij inwerkingtreding van die wet wordt overgenomen door de Minister van Economische Zaken (Agentschap Telecom) (zie onderdeel W, artikel 20.15a, tweede lid, van het wetsvoorstel). Die behandeling dient op grond van het in artikel XI voorgestelde tweede lid alsdan met inachtneming van de nieuw in werking getreden wet plaats te vinden, waarbij de lopende aanvraag in de terminologie van de verordening betrekking heeft op het verkrijgen van de status gekwalificeerde verlener voor vertrouwensdiensten betreffende het verlenen van gekwalificeerde certificaten voor elektronische handtekeningen.

Naast gevallen waarin een aanvraag door een certificatiedienstverlener is ingediend, kan een aanvraag zijn ingediend tot aanwijzing van een instelling die veilige middelen op overeenstemming beoordeeld met wettelijke eisen. De behandeling van aanvragen hiervoor vindt onder de huidige Telecommunicatiewet door de Minister van Economische Zaken plaats en dit blijft in het wetsvoorstel onveranderd. Het voorgestelde derde lid regelt het overgangsrecht voor een lopende aanvraag die hierop betrekking heeft.

Het in het vierde en vijfde lid voorgestelde overgangsrecht betreft voorts situaties van bezwaar of beroep waarvoor is bepaald dat het recht van toepassing is zoals dat gold voordat dit wetsvoorstel tot wet wordt verheven en in werking treedt. Dit houdt ook in dat voor bezwaar en beroep tegen besluiten op een aanvraag van een certificatiedienstverlener ACM het terzake bevoegde bestuursorgaan blijft voor bezwaar en beroep.

In het artikel wordt tot slot voorzien in de continuering van de aanwijzing van instellingen die veilige middelen op overeenstemming beoordelen met wettelijke eisen, zodat die niet hiervoor een nieuwe aanvraag hoeven in te dienen.

Artikel XII

Gelet op toepasselijkheid van de eidas-verordening vanaf 1 juli 2016 voor vertrouwensdiensten kan het beleid inzake vaste verandermomenten niet worden gevolgd, zowel ten aanzien van het moment van inwerkingtreding als het moment van publicatie.

III. Implementatietabel

Verordening 2014/910/EU	Telecommunicatiewet, Burgerlijk Wetboek en Algemene wet bestuursrecht	Omschrijving beleidsruimte	Toelichting op keuze bij invulling beleidsruimte
Artikel 1	Rechtstreekse werking volstaat.		
Artikel 2	Artikel I, onderdeel F (artikel 2.5a, Telecommunicatiewet)		
Artikel 3	Artikel I, onderdeel A (artikel 1.1, Telecommunicatiewet), alsmede artikelen VI, artikel VII, eerste lid, artikel VIII, artikel IX		

Verordening 2014/910/EU	Telecommunicatiewet, Burgerlijk Wetboek en Algemene wet bestuursrecht	Omschrijving beleidsruimte	Toelichting op keuze bij invulling beleidsruimte
Artikel 4	Rechtstreekse werking volstaat.		
Artikel 5, eerste en tweede lid	Artikel I, onderdeel G (artikel 11.5b, Telecommunicatiewet), artikel I, onderdeel F (artikel 2.5e, Telecommunicatiewet), artikel I, onderdeel Q (artikel 18.15ᵉ, Telecommunicatiewet) en paragraaf 8 van het algemeen deel van de memorie van toelichting.		
Artikel 6, eerste lid	Feitelijke uitvoering m.b.v. een technische voorziening, een knooppunt. Waarborging naleving op basis Wet Naleving Europese regelgeving publieke entiteiten.		
Artikel 6, tweede lid	Rechtstreekse werking volstaat.		
Artikel 7	Van mogelijkheid is (nog) geen gebruik gemaakt.	Mogelijkheid voor lidstaat stelsel voor elektronische identificatie aan te melden bij de Europese Commissie (zie tevens overweging 13 van de verordening).	De verplichte erkenning van aangemelde stelsels is van toepassing vanaf september 2018. Ten tijde van de totstandkoming van dit wetsvoorstel heeft besluitvorming over het aanmelden van een stelsel door Nederland nog niet plaatsgevonden. Reden hiervoor is dat het stelsel Idensys nog in ontwikkeling is.
Artikel 8, eerste en tweede lid	Rechtstreekse werking volstaat.		
Artikel 8, derde lid	De bepalingen richten zich tot de Europese Commissie		
Artikel 9, eerste lid	Rechtstreekse werking volstaat.		
Artikel 9, tweede en derde lid	De bepalingen richten zich tot de Europese Commissie		
Artikel 9, vierde lid	Rechtstreekse werking volstaat.		
Artikel 9, vijfde lid	De bepalingen richten zich tot de Europese Commissie		
Artikel 10	Rechtstreekse werking volstaat.		
Artikel 11, eerste tot en met derde lid	Rechtstreekse werking volstaat.		
Artikel 11, vierde en vijfde lid	Rechtstreekse werking volstaat. Regels inzake aansprakelijkheid zijn onderdeel van Boek 6 van het Burgerlijk Wetboek		
Artikel 12, eerste tot en met zesde lid	Rechtstreekse werking volstaat.		
Artikel 12, zevende tot en met negende lid	De bepalingen richten zich tot de Europese Commissie.		
Artikel 13, eerste en tweede lid	Artikel III (artikel 196b, van Boek 6 BW).		
Artikel 13, derde lid	Regels inzake aansprakelijkheid zijn onderdeel van Boek 6 van het Burgerlijk Wetboek		
Artikel 14	Artikel II, onderdeel B (artikel 15b van Boek 3 BW)		
Artikel 15	Rechtstreekse werking volstaat.		
Artikel 16	Bevoegdheden tot handhaving van naleving zijn gekoppeld aan het zijn van toezichthouder (Artikel I, onderdeel I (artikel 15.1, Telecommunicatiewet); voorts Wet naleving Europese regelgeving publieke entiteiten voor voorschriften gericht tot openbare instanties.		
Artikel 17, eerste lid, eerste volzin	Artikel I, onderdeel L (artikel 18.2a, tweede lid, Telecommunicatiewet)		



Verordening 2014/910/EU	Telecommunicatiewet, Burgerlijk Wetboek en Algemene wet bestuursrecht	Omschrijving beleidsruimte	Toelichting op keuze bij invulling beleidsruimte
Artikel 17, eerste lid, tweede volzin	Artikel I, onderdeel I (artikel 15.1, eerste lid, Telecommunicatiewet), onderdeel J (artikelen15.3b, tweede en derde lid en 15.3d, derde lid, Telecommunicatiewet), onderdeel M (artikel 18.3a, Telecommunicatiewet), onderdeel O (artikel 18.7, eerste lid, Telecommunicatiewet)		
Artikel 17, tweede lid	Feitelijke uitvoering.		
Artikel 17, derde lid	Rechtstreekse werking volstaat.		
Artikel 17, vierde lid, onderdeel a	Artikel I, onderdeel J (artikelen 15.3b tot en met 15.3d, Telecommunicatiewet)		
Artikel 17, vierde lid, onderdeel b	Artikel I, onderdeel Q		
Artikel 17, vierde lid, onderdeel c	Rechtstreekse werking volstaat.		
Artikel 17, vierde lid, onderdeel d	Rechtstreekse werking volstaat.		
Artikel 17, vierde lid, onderdeel e	Artikel I, onderdeel Q		
Artikel 17, vierde lid, onderdeel f	Rechtstreekse werking volstaat.		
Artikel 17, vierde lid, onderdeel g	Artikel I, onderdeel F (artikelen 2.5b en 2.5d, Telecommunicatiewet)		
Artikel 17, vierde lid, onderdeel h		Het toezichthoudend orgaan brengt het voor de nationale vertrouwenslijst verantwoordelijke orgaan op de hoogte van statustoekenning of -intrekking, tenzij dit orgaan ook het toezichthoudend orgaan is.	De Minister van Economische Zaken is verantwoordelijk voor de vertrouwenslijst en is tevens toezichthoudend orgaan. Hier is om pragmatische redenen voor gekozen en dit sluit ook aan bij de bestaande toezichtspraktijk.
Artikel 17, vierde lid, onderdeel i	Rechtstreekse werking volstaat.		
Artikel 17, vierde lid, onderdeel j	Artikel I, onderdeel I (artikel 15.1, Telecommunicatiewet)		
Artikel 17, vijfde lid	Van mogelijkheid is geen gebruik gemaakt.	Mogelijkheid dat het toezichthoudend orgaan een vertrouwensinfrastructuur opzet en onderhoudt	Dit sluit niet aan bij de huidige Nederlandse praktijk en hieraan uitvoering geven zou verder gaan dan voor minimumomzetting van de verordening vereist is.
Artikel 17, zesde lid	Rechtstreekse werking volstaat.		
Artikel 17, zevende en achtste lid	Bepaling richt zich tot de Europese Commissie.		
Artikel 18, eerste lid	Artikel I, onderdeel J (artikel 15.3b, Telecommunicatiewet)		
Artikel 18, tweede lid	Artikel I, onderdeel J (artikel 15.3c, Telecommunicatiewet)		
Artikel 18, derde lid	Artikel I, onderdeel J (artikel 15.3d, Telecommunicatiewet)		
Artikel 19, eerste lid	Behoeft naar zijn aard geen implementatie in wetgeving		
Artikel 19, tweede lid, eerste alinea	Artikel I, onderdeel H (artikel 11.5c, Telecommunicatiewet), onderdeel L (artikel 18.2a, tweede lid, Telecommunicatiewet), onderdeel Q (artikelen 18.15a. eerste lid en 18.15b, Telecommunicatiewet)		
Artikel 19, tweede lid, tweede alinea	Artikel I, onderdeel Q (artikel 18.15a. tweede lid, Telecommunicatiewet)		
Artikel 19, tweede lid, derde alinea	Rechtstreekse werking volstaat.		
Artikel 19, tweede lid, vierde alinea	Rechtstreekse werking volstaat.		
Artikel 19, derde lid	Rechtstreekse werking volstaat.		

Verordening 2014/910/EU	Telecommunicatiewet, Burgerlijk Wetboek en Algemene wet bestuursrecht	Omschrijving beleidsruimte	Toelichting op keuze bij invulling beleidsruimte
Artikel 19, vierde lid	Artikel I, onderdeel Q (artikelen 18.15a. eerste lid en 18.15b, Telecommunicatiewet)		
Artikel 20, eerste en tweede lid,	Artikel I, onderdeel R		
Artikel 20, derde lid	Artikel I, onderdeel F (artikel 2.5d, Telecommunicatiewet)		
Artikel 20, vierde lid	Bepaling richt zich tot Europese Commissie.		
Artikel 21, eerste lid	Artikel I, onderdeel F (artikel 2.5b) en R (Telecommunicatiewet)		
Artikel 21, tweede lid	Artikel I, onderdeel R (Telecommunicatiewet)		
Artikel 21, derde lid	Rechtstreekse werking volstaat. Voorts onderdeel U (artikel 18.18 van de Telecommunicatiewet)		
Artikel 21, vierde lid	Bepaling richt zich tot Europese Commissie.		
Artikel 22, eerste lid	Artikel I, onderdeel F (artikel 2.5c, Telecommunicatiewet)		
Artikel 22, tweede lid	Rechtstreekse werking volstaat.		
Artikel 22, derde lid	Artikel I, onderdeel F (artikel 2.5c, Telecommunicatiewet)		
Artikel 22, vierde lid	Bepaling richt zich tot Europese Commissie.		
Artikel 22, vijfde lid	Bepaling richt zich tot Europese Commissie.		
Artikel 23	Rechtstreekse werking volstaat.		
Artikel 24, eerste lid, aanhef en onder a	Artikel I, onderdeel Q (artikelen 18.15c, 18.15e, 18.15f, Telecommunicatiewet)		
Artikel 24, eerste lid, aanhef en onder b	Artikel I, onderdeel Q (artikelen 18.15d, eerste lid, 18.15e, 18.15f, Telecommunicatiewet)		
Artikel 24, eerste lid, aanhef en onder c	Artikel I, onderdeel Q (artikelen 18.15d, tweede lid, 18.15e, 18.15f, Telecommunicatiewet)		
Artikel 24, eerste lid, aanhef en onder d		Van mogelijkheid tot verificatie op basis van andere op nationaal niveau erkende identificatiemethoden is geen gebruik gemaakt	Gelet op het uitgangspunt van minimumomzetting van de verordening, is in het voorstel er vanaf gezien deze mogelijkheid nader te onderzoeken.
Artikel 24, tweede tot en met vierde lid	Artikel I, onderdeel P (artikel 18.15, Telecommunicatiewet)		
Artikel 24, vijfde lid	Bepaling richt zich tot Europese Commissie.		
Artikelen 25 en 26	Artikel II, onderdelen A en C (artikelen 15a en 15c, Boek 3 BW) en artikel V (artikel 2:16, Awb)		
Artikel 27, eerste en tweede lid	Feitelijke uitvoering voor openbare instanties mogelijk met behulp van valideringsdienst Ondernemersplein. Waarborgen naleving op basis van Wet naleving Europese regelgeving publieke entiteiten.		
Artikel 27, derde lid	Rechtstreekse werking volstaat. Voorts artikel VII (artikel 7e, Kadasterwet)		
Artikel 27, vierde en vijfde lid	Bepaling richt zich tot Europese Commissie.		
Artikel 28, eerste lid	Artikel I, onderdeel P (artikel 18.15, Telecommunicatiewet)		
Artikel 28, tweede tot en met vierde lid	Rechtstreekse werking volstaat.		

Verordening 2014/910/EU	Telecommunicatiewet, Burgerlijk Wetboek en Algemene wet bestuursrecht	Omschrijving beleidsruimte	Toelichting op keuze bij invulling beleidsruimte
Artikel 28, vijfde lid		Van mogelijkheid tot vaststellen regels inzake tijdelijke schorsing gekwalificeerd certificaat voor elektronische handtekeningen is geen gebruik gemaakt.	In Nederland wordt van de mogelijkheid tot het opschorten van certificaten geen gebruik gemaakt. Er is geen behoefte om deze lijn te wijzigen. In het (private) programma van eisen PKI-overheid is vastgelegd dat het niet toegestaan is certificaatopschorting te ondersteunen.
Artikel 28, zesde lid	Bepaling richt zich tot Europese Commissie.		
Artikel 29, eerste lid	Artikel I, onderdeel P (artikel 18.15, Telecommunicatiewet)		
Artikel 29, tweede lid	Bepaling richt zich tot Europese Commissie		
Artikel 30, eerste lid	Onderdelen S (artikel 18.17, Telecommunicatiewet) en T (artikel 18.17a, Telecommunicatiewet)		
Artikel 30, tweede lid	Rechtstreekse werking volstaat.		
Artikel 30, derde lid	Onderdeel T (artikel 18.17a, Telecommunicatiewet)		
Artikel 30, vierde lid	Bepaling richt zich tot Europese Commissie		
Artikel 31, eerste lid	Onderdeel T (artikel 18.17a, zesde en zevende lid, Telecommunicatiewet)		
Artikel 31, tweede en derde lid	Bepaling richt zich tot de Europese Commissie.		
Artikel 32, eerste en tweede lid	Rechtstreekse werking volstaat.		
Artikel 32, derde lid	Artikel I, onderdeel P (artikel 18.15, onder a, van de Telecommunicatiewet)	Indien Commissie geen referentienummers vaststelt, dan mogelijkheid dit nationaal te doen.	Vanuit het belang van veiligheid is het wenselijk nationaal referentienummers vast te stellen, zolang de Europese Commissie hierin niet voorziet.
Artikel 33, eerste lid	Rechtstreekse werking volstaat		
Artikel 33, tweede lid	Artikel I, onderdeel P (artikel 18.15, onder a, van de Telecommunicatiewet)	Indien Commissie geen referentienummers vaststelt, dan mogelijkheid dit nationaal te doen.	Vanuit belang van veiligheid is het wenselijk nationaal referentienummers vast te stellen, zolang de Europese Commissie hierin niet voorziet.
Artikel 34, eerste lid	Rechtstreekse werking volstaat		
Artikel 34, tweede lid	Artikel I, onderdeel P (artikel 18.15, onder a, van de Telecommunicatiewet)	Indien Commissie geen referentienummers vaststelt, dan mogelijkheid dit nationaal te doen.	Vanuit belang van veiligheid is het wenselijk nationaal referentienummers vast te stellen, zolang de Europese Commissie hierin niet voorziet.
Artikel 35	Rechtstreekse werking volstaat		
Artikel 36	Rechtstreekse werking volstaat		
Artikel 37, eerste tot en met derde lid	Rechtstreekse werking volstaat; Wet Naleving Europese regelgeving publieke entiteiten		
Artikel 37, vierde en vijfde lid	Bepaling richt zich tot de Europese Commissie		
Artikel 38, eerste tot en met vierde lid	Rechtstreekse werking volstaat		

Verordening 2014/910/EU	Telecommunicatiewet, Burgerlijk Wetboek en Algemene wet bestuursrecht	Omschrijving beleidsruimte	Toelichting op keuze bij invulling beleidsruimte
Artikel 38, vijfde lid	Van mogelijkheid geen gebruik gemaakt.	Mogelijkheid voor lidstaten nationale regels vast te stellen inzake tijdelijke schorsing van gekwalificeerde certificaten voor elektronische zegels	In Nederland wordt van de mogelijkheid tot het opschorten van certificaten geen gebruik gemaakt. Er is geen behoefte om deze lijn te wijzigen. In het (private) programma van eisen PKI-overheid is vastgelegd dat het niet toegestaan is certificaatopschorting te ondersteunen.
Artikel 38, zesde lid	Artikel I, onderdeel P (Artikel 18.15, onder a, van de Telecommunicatiewet)	Indien Commissie geen referentienummers vaststelt, dan mogelijkheid dit nationaal te doen.	Vanuit belang van veiligheid is het wenselijk nationaal referentienummers vast te stellen, zolang de Europese Commissie hierin niet voorziet.
Artikel 39, eerste lid	Artikel I, onderdeel P (artikel 18.15, onder b, van de Telecommunicatiewet)	Indien Commissie geen referentienummers vaststelt, dan mogelijkheid dit nationaal te doen.	Vanuit belang van veiligheid is het wenselijk nationaal referentienummers vast te stellen, zolang de Europese Commissie hierin niet voorziet.
Artikel 39, tweede lid	Artikel I, onderdelen S (artikel 18.17, Telecommunicatiewet) en T (artikel 18.17a, Telecommunicatiewet)		
Artikel 39, derde lid	Artikel I, onderdeel T (artikel 18.17a, zesde en zevende lid, Telecommunicatiewet)		
Artikel 40	Artikel I, onderdeel P, (artikel 18.15, onder a, van de Telecommunicatiewet)	Indien Commissie geen referentienummers vaststelt, dan mogelijkheid dit nationaal te doen.	Vanuit belang van veiligheid is het wenselijk nationaal referentienummers vast te stellen, zolang de Europese Commissie hierin niet voorziet.
Artikel 41	Rechtstreekse werking volstaat.		
Artikel 42, eerste lid	Rechtstreekse werking volstaat.		
Artikel 42, tweede lid	Artikel I, onderdeel P (artikel 18.15, onder a, van de Telecommunicatiewet)	Indien Commissie geen referentienummers vaststelt, dan mogelijkheid dit nationaal te doen.	Vanuit belang van veiligheid is het wenselijk nationaal referentienummers vast te stellen, zolang de Europese Commissie hierin niet voorziet.
Artikel 43	Rechtstreekse werking volstaat.		
Artikel 44, eerste lid	Rechtstreekse werking volstaat.		
Artikel 44, tweede lid	Artikel I, onderdeel P (artikel 18.15, onder a, van de Telecommunicatiewet)	Indien Commissie geen referentienummers vaststelt, dan mogelijkheid dit nationaal te doen.	Vanuit belang van veiligheid is het wenselijk nationaal referentienummers vast te stellen, zolang de Europese Commissie hierin niet voorziet.
Artikel 45, eerste lid	Rechtstreekse werking volstaat.		
Artikel 45, tweede lid	Artikel I, onderdeel P (artikel 18.15, onder a, van de Telecommunicatiewet)	Indien Commissie geen referentienummers vaststelt, dan mogelijkheid dit nationaal te doen.	Vanuit belang van veiligheid is het wenselijk nationaal referentienummers vast te stellen, zolang de Europese Commissie hierin niet voorziet.
Artikel 46	Rechtstreekse werking volstaat.		
Artikel 47	Bepalingen richten zich tot de Europese Commissie.		
Artikel 48	Bepalingen richten zich tot de Europese Commissie.		
Artikel 49	Bepalingen richten zich tot de Europese Commissie.		
Artikel 50	Rechtstreekse werking volstaat.		
Artikel 51	Rechtstreekse werking volstaat (zie paragraaf 9.2 van het algemeen deel van de memorie van toelichting)		
Artikel 52	Rechtstreekse werking volstaat.		



Verordening 2014/910/EU	Telecommunicatiewet, Burgerlijk Wetboek en Algemene wet bestuursrecht	Omschrijving beleidsruimte	Toelichting op keuze bij invulling beleidsruimte
Bijlage I	Rechtstreekse werking volstaat.		
Bijlage II	Rechtstreekse werking volstaat.		
Bijlage III	Rechtstreekse werking volstaat.		
Bijlage IV	Rechtstreekse werking volstaat.		

De Minister van Economische Zaken,